Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice* forthcoming)
lpittman@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Facsimile: 415.956.1008

Jason "Jay" O. Barnes (*pro hac vice* forthcoming)
jaybarnes@simmonsfirm.com
An V. Truong (*pro hac vice* forthcoming)
atruong@simmonsfirm.com
Sona R. Shah (*pro hac vice* forthcoming)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: 212.784.6400
Facsimile: 212.213.5949

Attorneys for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CHRISTINE RIGANIAN and DONNA SPURGEON, *on behalf of themselves and all others similarly situated,*

Plaintiffs,

v.

LIVERAMP HOLDINGS INC., *a corporation organized under the laws of the State of Delaware,*

Defendant.

Case No. 3:25-cv-824

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

I. INTRODUCTION 1
II. PLAINTIFFS 5
A. Plaintiff Christina Riganian 5
1. LiveRamp's Comprehensive Identity Profile on Plaintiff Riganian 5
2. LiveRamp's Interception and Use of Plaintiff Riganian's Online Browsing Activity 7
B. Plaintiff Donna Spurgeon 10
1. LiveRamp's Comprehensive Identity Profile on Plaintiff Spurgeon 10
2. LiveRamp's Interception and Use of Plaintiff Spurgeon's Online Browsing Activity 11
III. DEFENDANT 13
IV. JURISDICTION AND VENUE 13
V. CHOICE OF LAW 13
VI. DIVISIONAL ASSIGNMENT 14
VII. STATEMENT OF FACTS 14
A. LiveRamp Collects, Buys, and Analyzes Vast Amounts of On- and Offline Data to Track Individual Consumers Everywhere on the Internet and in the Real World. 14
1. LiveRamp Collects, Buys, and Analyzes Vast Amounts of Offline Data to Construct Real-World Identity Profiles Using Its AbiliTec System. 18
2. LiveRamp Collects, Buys, and Analyzes Vast Amounts of Online Data to Track Real-World Consumers' Digital Activities Using the RampID Identity Graph System. 21
B. Through "Data Onboarding," and Identity Resolution, LiveRamp and Its Customers Target Class Members Wherever They Are in the Digital and Physical Worlds. 27
C. Through "Authenticated Traffic Solutions" or "ATS," LiveRamp Enables Privacy-Invasive "Real-Time Bidding" Based on Class Members' Real-World Identities. 29
D. Through Its Data Marketplace, LiveRamp Facilitates the Sale of Vast Amounts of Sensitive Personal Information About Consumers and Facilitates the Construction of Detailed Consumer Profiles. 31
E. LiveRamp's "Third-Party Attribute Data Append" Is a Uniquely Invasive and Comprehensive Form of Surveillance. 38
F. LiveRamp's Practices are Recognized as Highly Offensive and Threats to Individual Privacy. 40

TABLE OF CONTENTS
(continued)

Page

G. Effective Consent to LiveRamp's Practices is Impossible. 47

VIII. CLASS ALLEGATIONS 52

IX. CAUSES OF ACTION 55

First Cause of Action Invasion of Privacy Under the California Constitution (on behalf of the California Sub-Class) 55

Second Cause of Action Intrusion Upon Seclusion Under California Common Law (on behalf of the United States Class) 59

Third Cause of Action Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630 to 638 (on behalf of the CIPA Sub-Class) 64

Fourth Cause of Action Violation of the Federal Wiretap Act, 18 U.S.C. § 2510, et. seq. (on behalf of the ECPA Sub-Class) 69

Fifth Cause of Action Unjust Enrichment under California Common Law (on behalf of the United States Class, or in the alternative on behalf of the California Sub-Class) 75

Sixth Cause of Action Declaratory Judgment that LiveRamp Wrongfully Accessed, Collected, Stored, Disclosed, Sold, and Otherwise Improperly Used Plaintiffs' Personal Information and Injunctive Relief (on behalf of all Classes) 77

X. PRAYER FOR RELIEF 78

XI. DEMAND FOR JURY TRIAL 79

I. INTRODUCTION

1. Americans do not expect that as they go about their daily lives they are being constantly tracked, surveilled, and manipulated by third parties with whom they never directly interact. Defendant LiveRamp Holdings, Inc. ("LiveRamp") engages in and profits from precisely such conduct by operating a massive identity surveillance system that assigns every American a proprietary, permanent identifier—the equivalent of an online social security number—which is tied to personal information such as names, postal addresses, email addresses, phone numbers, and to digital IDs referring to browsers and user accounts at online services, smartphones, and other devices associated with that person. LiveRamp uses its systems to profit from Americans' nearly every move online and offline, selling that information to third parties so that they may further surveil and manipulate people.

2. This complaint sets forth how the regularly conducted business practices of LiveRamp amount to the deliberate and purposeful surveillance of the general American population via their digital and online existence. As a worldwide data broker and identity resolution provider, LiveRamp has created a network that tracks *in real time* and records *indefinitely* the personal information of hundreds of millions of people. LiveRamp sells this detailed personal information to third parties through its "RampID" identity graph system, "Data Marketplace," and other related products and services derived from this data. The proposed Classes herein lack a direct relationship with LiveRamp and have no reasonable or practical basis upon which they could legally consent to LiveRamp's surveillance.

3. LiveRamp's business involves the maintenance of vast databases of personal information, from postal addresses and phone numbers to email addresses and electronic device and smartphone identifiers. LiveRamp infers connections between these pieces of information, linking them with "pseudonymous" (*i.e.*, not truly anonymous, but only partially obfuscated) identifiers so that with just one piece of information—a device identifier or email address for example—a comprehensive identifying profile of an individual can be retrieved. Its databases are in effect ***private population registers***: they contain the names, addresses, phone numbers, digital and device

identifiers, and electronic identity information for virtually every adult in the United States, updated in real time.

4. LiveRamp sells this functionality to a wide range of online actors, allowing them to monitor individuals as they browse, and to communicate with other online actors about individuals—most particularly individuals whom they want to, or allow other entities to, track, profile, and manipulate. In this way, LiveRamp's processing plays a major role in the worldwide commercial surveillance ecosystem.[1] LiveRamp also enables other data brokers to sell personal information about millions of people to data buyers, who can then further transmit records to other companies, all while ensuring the commercial actors in the chain are talking about the same individuals.

5. LiveRamp partners with the largest companies in the world to effect its massive surveillance network. For example, Google, Amazon, Meta, TikTok, and Microsoft are all LiveRamp "partners" that use LiveRamp's surveillance systems to track and manipulate people.[2] LiveRamp's conduct is uniquely invasive precisely because it allows for such wide-scale sharing and use of personal information amongst many actors.

6. LiveRamp maintains "the largest and most accurate people-based identity graph on the market," purportedly containing detailed personal information on 700 million consumers globally.[3] An "identity graph is" a "people-based map" connecting "offline touchpoints and online

[1] As defined by the Federal Trade Commission, "Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Technologies essential to everyday life also enable near constant surveillance of people's private lives. The volume of data collected exposes people to identity thieves and hackers. Mass surveillance has heightened the risks and stakes of errors, deception, manipulation, and other abuses." *See Commercial Surveillance and Data Security Rulemaking*, FEDERAL TRADE COMMISSION (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking [https://perma.cc/7DDW-SL7L].

[2] *See How to Use*, LIVERAMP ACTIVATION, https://developers.liveramp.com/activation-api/v1.1/reference/guide [https://perma.cc/85VG-VV59].

[3] *Interpreting RampID, LiveRamp's People-Based Identifier*, LIVERAMP, *https*://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [https://perma.cc/LC62-K3V2]; LiveRamp, Form 10-K (Mar. 31, 2021), https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [https://perma.cc/KFM8-8KWQ].

devices"—in other words, it is a map that connects "offline" information about people, such as their name, home address, and phone number, with their "online" devices such as web browsers, mobile phones, tablets, smart or "connected" TVs, and gaming consoles.[4] LiveRamp's identity graph connects all these identifying points of data into a single, non-anonymous "identity profile" connected to a real person that can be used to track all of that person's online activity in real time. As one commentator described it, "LiveRamp has created what is probably the world's most complete shadow identity system, with detailed profiles for a large proportion of the world's online users."[5]

7. While individuals generally know nothing about LiveRamp, LiveRamp knows an enormous amount about them. LiveRamp's business is to collect, process, and sell this individual-level data to other data brokers or businesses, allowing them to track, follow, profile, and target people across the digital online and offline worlds. LiveRamp's clients can, in turn, buy and sell personal information through "segments" (*i.e.*, lists of identifiers associated with people sharing certain characteristics) via LiveRamp's "Data Marketplace."[6] As recently reported, LiveRamp's clients buy and sell "segments" of digital identifiers associated with people's highly sensitive health, religious, economic, sexual, and financial information; LiveRamp makes or has made available for sale segments of people with cancer, union members, Muslims, Jewish people, African Americans, poor people, payday loan prospects, online gamblers, unemployed individuals who were "seen at clinics/hospitals" and users of the LGBT dating app Grindr.[7]

---

[4] *RampID Methodology*, LIVERAMP, https://docs.liveramp.com/identity/en/rampid-methodology.html [https://perma.cc/8WFU-C2JA].

[5] Glyn Moody, *This Global Identity System Tracks Everything You Do Online*, PRIVATE INTERNET ACCESS (Mar. 12, 2024), https://www.privateinternetaccess.com/blog/global-identity-system-tracks-you/ [https://perma.cc/VJ6Y-M48J].

[6] *Selling Data with the Data Marketplace*, LIVERAMP, https://docs.liveramp.com/connect/en/selling-data-with-the-data-marketplace.html [https://perma.cc/9XJB-9KYA].

[7] Jon Keegan and Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you [https://perma.cc/MUG2-N38J]. The Xandr spreadsheet file is available at: https://web.archive.org/web/20230525225541mp_/https://xandr-be-

8. This Data Marketplace could not exist without LiveRamp's vast identity graph system, "RampID," and "identity resolution services." "Identity resolution" refers to the process of merging or "resolving" various distinct pieces of personal information or "touchpoints" (an email address, physical address, and a mobile device ID, for example) into a comprehensive "identity profile" of a single person, facilitated by LiveRamp's identity graph systems.

9. All of this is done without consumers' consent or even their awareness that it is happening. The breadth and complexity of methods and sources by which LiveRamp collects personal information to compile digital dossiers, or comprehensive identity profiles, on consumers is such that as a practical matter, consumers have no way of knowing—let alone being able to consent to—LiveRamp's conduct. Consumers do not, merely by virtue of conducting the necessary activities of daily life, both online and offline, consent to LiveRamp's creation of comprehensive identity profiles about them and the company's constant and pervasive surveillance.

10. LiveRamp's processing is complex, and the way its business model works is opaque and difficult to understand for ordinary consumers, including Plaintiffs. LiveRamp's conduct as described herein is such that individuals engaging in virtually any online activity can be tracked and influenced in a personalized way without them realizing it. Indeed, even where a person employs internet usage behaviors that they might think protect them from being tracked—for example, not logging into sites, or only providing partial contact information—they can be monitored and profiled in ways they would not expect as a result of LiveRamp's practices described herein.

11. LiveRamp's data coffers contain vast repositories of personal information compiled from Plaintiffs' browsing activity, online communications, and offline, real-world activity, which LiveRamp offers for sale to third parties. As one well-known security researcher described it, "LiveRamp is like a stalker, who gradually learns more about the target, but it's highly automated, at population scale, and it sells this stalking ability to many other companies."[8]

---

prod.zoominsoftware.io/bundle/monetize_monetize-standard/page/attachments/data-marketplace-buyer-overview/data_marketplace_public_segments_pricing_05212021.xlsx.

[8] Wolfie Christl, quoted in John Leonard, *'Like a stalker': Data Broker LiveRamp Reported to UK, French Regulators*, COMPUTING (Mar. 4, 2024), https://www.computing.co.uk/news/4180665/stalker-broker-liveramp-reported-uk-french-regulators [https://perma.cc/2GG3-NG4W].

12. Plaintiffs are concerned citizens who believe that LiveRamp's identity surveillance technologies abrogate Americans' privacy and autonomy. Plaintiffs bring this action to enforce their fundamental right to privacy, seek redress and compensation for the financial, dignitary, and relational harms LiveRamp has caused, and obtain a ruling that LiveRamp's conduct is unlawful and therefore must stop. The law, as alleged below, entitles Plaintiffs and the proposed Classes to these remedies.

II. PLAINTIFFS

A. Plaintiff Christina Riganian

13. Plaintiff Christina Riganian is a resident of Tujunga, California. Like most members of modern society, Plaintiff Riganian must use the Internet to conduct routine affairs of daily life.

1. LiveRamp's Comprehensive Identity Profile on Plaintiff Riganian

14. On September 13, 2024, Plaintiff Riganian received a "Subject Access Request" (SAR)[9] from LiveRamp indicating that LiveRamp has created a massive and comprehensive identity profile on her. The SAR consists of 18 separate "excel" spreadsheet files that purportedly reflect the information LiveRamp collected and processed on her. These files collectively contain *several thousand* pieces of information about Plaintiff Riganian. Based on a reasonable investigation of these files and the explanatory information made available by LiveRamp:

a. **"names_and_phones" and "names_and_postals"**: These two files contains almost every address where Plaintiff Riganian has lived since 1992, when she was a child, and every phone number that has been associated with her for the last twenty years.

b. **"names_and_emails"**: This file contains years' worth of electronic identifiers associated with her, including email addresses she has used for at least the last twenty years.

c. **"ps_links"**: LiveRamp also collected and associated over six hundred cookies and unique device identifiers, and hashed email-associated identifiers, with the profile it maintains on her.

[9] Out of respect for Plaintiff Riganian's privacy, the SAR is not attached to this Complaint but is incorporated by reference herein.

d. "**mobile_links**": This file demonstrates LiveRamp collected and associated with Plaintiff Riganian over one hundred unique "mobile advertising IDs" that were associated with her mobile devices.

e. "**cid_links**": This file demonstrates that LiveRamp collected and associated with its internal profile on Plaintiff Riganian hundreds of "Custom IDs" ("CIDs") from "various partners [LiveRamp] work[s] with."[10] CIDs are "typically persistent and assigned to you when you create an account with our partners e.g. a social media network, subscription service, or rewards program for retailers." In other words, LiveRamp collected identifiers associated with Plaintiff Riganian from hundreds of third parties across the internet in order to enrich its internal identity dossier on Plaintiff Riganian.

f. "**mobile_pel_requests**": This file contains a log of over 1,800 instances over the last four years in which a LiveRamp pixel was deposited on one of Plaintiff Riganian's devices. The vast majority of these—nearly 1,400—were deposited in the last year, averaging almost 4 incidents a day. Because of the deliberately obfuscatory and incomplete nature of the information LiveRamp provides in this file, Plaintiffs cannot determine the websites, mobile apps, or third parties these pixels are associated with. On information and belief, these pixels represent at least some instances of LiveRamp's deployment of the wiretapping mechanisms described below on Plaintiff Riganian's devices.

g. "**ThirdPartyAccessList**": This file contains a (potentially incomplete)[11] list of the "specific third parties to which LiveRamp has disclosed [Plaintiff Riganian's] personal data."[12] The csv file discloses that LiveRamp shared Plaintiff Riganian's personal information with at least 62 third parties, including pharmaceutical companies (AbbVie), publishers (*e.g.*, USA Today, Future plc), advertisers (*e.g.*, Hewlett Packard, Kraft),

[10] Data Subject Access Request Explanatory Information Document Consumer Data at 8, version 3.2, LIVERAMP (May 31, 2024).

[11] *Id.* at 14 (LiveRamp states that it may withhold the names of some third parties with which it has shared data: "Some third parties may be withheld because the customer list is a trade secret.").

[12] *Id.*

AdTech firms and intermediaries (*e.g.*, Freewheel, a Comcast subsidiary), AdTech giants (*e.g.*, Google, Amazon, Microsoft), and also data brokers who sell third-party data via LiveRamp's Data Marketplace (*e.g.*, Lotame, IRI). This file thus demonstrates the sheer scope of LiveRamp's surveillance and information-sharing network, which disseminated Plaintiff Riganian's personal information across the internet and made it available to potentially thousands of additional parties who may then trade in or resell Plaintiff Riganian's personal information.

15. The SAR contains nearly a dozen additional files, demonstrating LiveRamp's tracking of Plaintiff Riganian's online activity through various companies such as smart-TV maker Vizio, audio streaming service Pandora, tech giant Amazon, and other AdTech companies and data brokers.

16. The SAR also discloses that LiveRamp has assigned to Plaintiff Riganian inescapable and persistent "RampIDs"—the equivalent of a universal "online social security number" used to track, profile, and persistently surveil her, as described in detail below.

17. The SAR further discloses that LiveRamp has collected and maintains in its identity resolution systems two of the most sensitive pieces of information about Plaintiff Riganian—her social security number and her driver's license data—and has used that information to permanently identify her. LiveRamp admits that it "collect[s] Social Security Number and Driver's License data associated with US residents" and that "[t]his data is used internally for identity resolution purposes."[13]

2. LiveRamp's Interception and Use of Plaintiff Riganian's Online Browsing Activity

18. LiveRamp continues to track Plaintiff Riganian's online and offline activity, enrich the profile on her as described below, and make her personal information available to third parties without her consent. Plaintiff Riganian has visited websites where her electronic communications were intercepted by the use of LiveRamp code, as described below.

[13] *Id.* at 7.

19. The full scope and extent of LiveRamp's tracking and compiling of Plaintiff Riganian's online and offline activity and personal information resides with LiveRamp itself, is not fully disclosed by LiveRamp, and therefore must be determined through discovery from LiveRamp. Based on a reasonable investigation, Plaintiff Riganian alleges as follows:

20. LiveRamp has tracked Plaintiff Riganian's activity on at least hundreds of websites and mobile apps, including the interception and collection of Plaintiff's searches for and views of articles related to health and personal financial issues on numerous websites. LiveRamp tracking mechanisms—including "cookies," "pixels," or JavaScript code—as described below at paragraphs 74–79, were present on those websites.

21. Those tracking mechanisms transmitted to LiveRamp the URL data, coupled with unique identifiers that LiveRamp used to associate browsing history with other data, compiled into a data profile about Plaintiff Riganian. LiveRamp's wiretapping and pen register code—which transmits to LiveRamp domains "di.rlcdn.com" and "ats.rlcdn.com"—was present on a subset of websites visited by Plaintiff, which, in turn, transmitted to LiveRamp the content of Plaintiff's communications and interactions with the websites, including the precise articles read, products viewed, as well as routing, addressing or signaling information related to these online interactions. LiveRamp maintains a data profile concerning Plaintiff Riganian, to which LiveRamp provides direct or indirect access (*e.g.*, via products or services derived from the profile) to at least dozens of third parties. LiveRamp engaged in this conduct throughout the class period.

22. For example, Plaintiff Riganian visited the website CVS.com to view information on specific conditions and medications. Plaintiff Riganian browsed to a URL substantially similar to this one:[14]

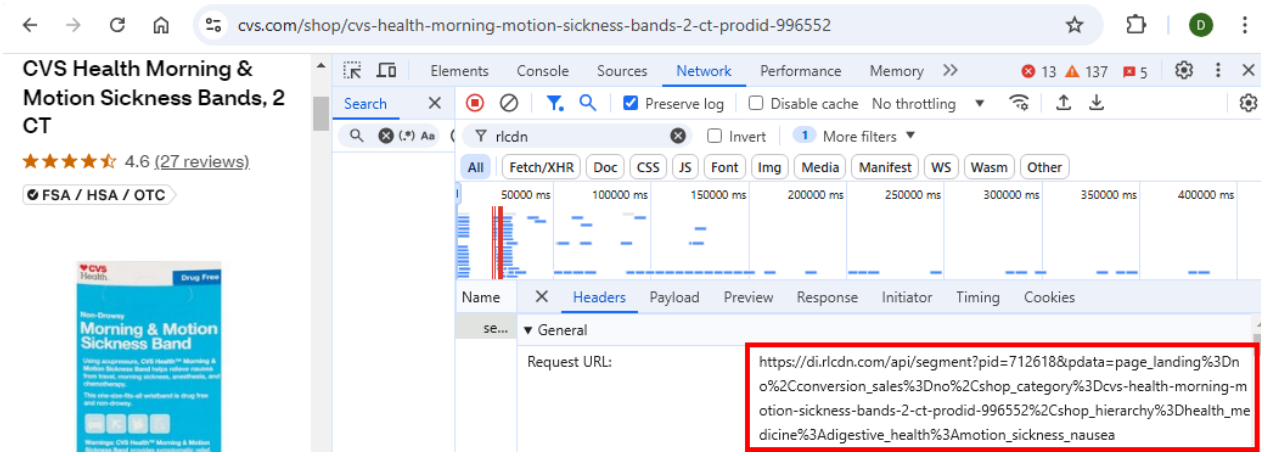
> https://www.cvs.com/shop/nauzene-upset-stomach-relief-chewable-tablets-42-ct-prodid-459986

23. On CVS.com, LiveRamp's eCST (enhanced client-side tag)—described in detail in Section VII.A.2. below—is deployed. It is configured to intercept contents of communications,

[14] To protect Riganian's health privacy, the specific URL she browsed to on the CVS.com website is not used an example.

encoded in LiveRamp's systems as "pdata," including the full URL revealing the specific item viewed by the website user, as illustrated by the following URL, with the precise drug being viewed sent to LiveRamp ("pdata" indicated in bold):

> https://di.rlcdn.com/api/segment?pid=712618&**pdata**=page_landing%3Dno%2Cconversion_sales%3Dno%2C**shop_category**%3Dcvs-**health-morning-motion-sickness-bands-2-ct-prodid-996552**%2C**shop_hierarchy**%3D**health_medicine** %3A**digestive_health** %3A**motion_sickness_nausea**



24. The LiveRamp trackers on the CVS.com website are configured to intercept and simultaneously transmit to LiveRamp the full URL of the products viewed.

25. Additionally, LiveRamp captures "segment" and "category" information related to these products—such as "health medicine," "digestive health," and "motion sickness nausea" in the example above—and associates Plaintiff Riganian with these "segments" and "categories," thereby adding to the information LiveRamp has compiled on her. On information and belief, these segments and categories—which reflect specific medications and conditions Plaintiff Riganian searched for on CVS.com, were made available for sale through LiveRamp, either directly through its "Data Marketplace" or otherwise facilitated by LiveRamp's systems, described in detail below.

26. The websites visited by Plaintiff Riganian where LiveRamp's tracking mechanisms have been detected include but are not limited to:

a. Healthline.com

b. CVS.com

c. Health.usnews.com

d. Goodrx.com

e. LAtimes.com

27. Additionally, LiveRamp's tracking mechanisms—in particular cookies—were located on Plaintiff Riganian's devices. These cookies were associated with Plaintiff Riganian's visits to the website hulu.com and a banking website.[15]

28. On information and belief, LiveRamp also offers for sale detailed and highly sensitive personal information on Plaintiffs through its Data Marketplace. LiveRamp claims to "offer multi-sourced insight into approximately 700 million consumers worldwide"[16] through its Data Marketplace, fueled by permanent "RampID" internet identification numbers assigned to these people, including Plaintiff Riganian. The full extent and nature of the personal information related to Plaintiff Riganian bought and sold on the Data Marketplace is unknown to her.

B. Plaintiff Donna Spurgeon

29. Plaintiff Donna Spurgeon is a resident of Lowell, Oregon, and previously a resident of Ojai, California. Like most members of modern society, Plaintiff Spurgeon must use the Internet to conduct routine affairs of daily life, including managing her financial, medical, and personal affairs.

1. LiveRamp's Comprehensive Identity Profile on Plaintiff Spurgeon

30. On January 12, 2024, Plaintiff Spurgeon received a "Subject Access Request" (SAR)[17] from LiveRamp indicating that LiveRamp has created a massive and comprehensive identity profile on her. The SAR consists of 9 separate "excel" spreadsheet files that purportedly reflect the information LiveRamp collected and processed on her. These files collectively contain hundreds of lines of information about Plaintiff Spurgeon. Based on a reasonable investigation and the explanatory information made available by LiveRamp, these files provide as follows:

[15] Banking website not named to protect Plaintiff Riganian's financial privacy.

[16] LiveRamp, Form 10-K, at 12 (Mar. 31, 2021), https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [https://perma.cc/KFM8-8KWQ].

[17] Out of respect for Plaintiff Spurgeon's privacy, the SAR is not attached to this Complaint but is incorporated by reference herein.

a. **"names_and_phones" and "names_and_postals"**: These two files contain almost every address she has lived at and every phone number that has been associated with her for at least the last twenty-five years.

b. **"names_and_emails"**: This file contains years' worth of electronic identifiers associated with her, including email addresses she has used for at least the last fourteen years.

c. **"ps_links"**: LiveRamp also collected and associated with the profile it maintains on her dozens of cookies and unique device and advertising identifiers.

31. The SAR also discloses that LiveRamp has assigned to Plaintiff Spurgeon an inescapable and persistent "RampID"—the equivalent of a universal "online social security number" used to track, profile, and persistently surveil her, as described in detail below.

32. The SAR also demonstrates that LiveRamp has collected and maintains in its identity resolution systems two of the most sensitive pieces of information about Plaintiff Spurgeon—her social security number and her driver's license data—and has used that information to permanently identify her. LiveRamp admits that it "collect[s] Social Security Number and Driver's License data associated with US residents" and that "[t]his data is used internally for identity resolution purposes."[18]

2. LiveRamp's Interception and Use of Plaintiff Spurgeon's Online Browsing Activity

33. LiveRamp continues to track Plaintiff Spurgeon's online and offline activity, enrich the profile on her as described below, and make her personal information available to third parties without her consent. Plaintiff Spurgeon has visited websites where her electronic communications were intercepted by the use of LiveRamp code, as described below.

34. The full scope and extent of LiveRamp's tracking and compiling of Plaintiff Spurgeon's online and offline activity and personal information resides with LiveRamp itself, is not fully disclosed by LiveRamp, and therefore must be determined through discovery from LiveRamp. Based on a reasonable investigation, Plaintiff Spurgeon alleges as follows:

[18] Data Subject Access Request Explanatory Information Document Consumer Data at 7, version 3.2, LIVERAMP (May 31, 2024).

35. LiveRamp has tracked Plaintiff Spurgeon's activity on at least hundreds of websites, including the interception and collection of Plaintiff's searches for and views of articles related to health and personal financial issues on numerous websites. LiveRamp tracking mechanisms—including "cookies," "pixels," and JavaScript code—as described below at paragraphs 74–79, were present on those websites.

36. Those tracking mechanisms transmitted URL data to LiveRamp, coupled with unique identifiers that LiveRamp used to associate browsing history with other data, compiled into a data profile about Plaintiff Spurgeon. LiveRamp's wiretapping and pen register code—which transmits to LiveRamp domains "di.rlcdn.com" and "ats.rlcdn.com"—was present on a subset of websites visited by Plaintiff, which, in turn, transmitted to LiveRamp the content of Plaintiff's communications and interactions with the websites, including the precise articles read, products viewed, and searches queried as well as routing, addressing or signaling information related to these online interactions. LiveRamp maintains a data profile concerning Plaintiff Spurgeon, to which LiveRamp provides direct or indirect access (*e.g.*, via products or services derived from the profile) to unknown third parties. LiveRamp engaged in this conduct throughout the class period.

37. The websites visited by Plaintiff Spurgeon where LiveRamp's tracking mechanisms have been detected include but are not limited to:

a. Healthline.com

b. CVS.com

c. Abcnews.go.com

d. Patient.info

e. Svu.edu

f. Health.usnews.com

g. Showtime.com

38. On information and belief, LiveRamp also offers for sale detailed and highly sensitive personal information on Plaintiff Spurgeon through its Data Marketplace, described in detail below. LiveRamp claims to "offer multi-sourced insight into approximately 700 million consumers worldwide" through its Data Marketplace, fueled by permanent "RampID" internet

identification numbers assigned to these people, including Plaintiff Spurgeon, as described in detail below. The full extent and nature of the personal information related to Plaintiff Spurgeon bought and sold on the Data Marketplace is unknown to her.

III. DEFENDANT

39. LiveRamp is a United States public corporation incorporated under the laws of the State of Delaware and is registered with the State of California under California Civil Code § 1798.99.80 as a "data broker."

40. LiveRamp's principal place of business is 225 Bush Street, 17th Floor, San Francisco, California 94104.

IV. JURISDICTION AND VENUE

41. This Court has jurisdiction over the subject matter of this case under 28 U.S.C. § 1331, because it arises under the laws of the United States, namely 18 U.S.C. ch. 119, and under 28 U.S.C. § 1367, because Plaintiffs' nonfederal claims share a common nucleus of operative fact with their federal claims.

42. This Court has jurisdiction over the subject matter of this case under 28 U.S.C. § 1332(d), because it is a putative class action in which at least one member of the putative classes is a citizen of a different state than LiveRamp, and in which the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000.

43. This Court has personal jurisdiction over LiveRamp, because LiveRamp is at home in California and because the claims arise from LiveRamp's conduct in California.

44. Venue lies in this District under 28 U.S.C. § 1391(b)(1) and (b)(2), because LiveRamp resides in this District, and because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

V. CHOICE OF LAW

45. California law governs the substantive legal issues in this case. The State of California has a significant interest in regulating the conduct of businesses operating within its borders.

46. LiveRamp's principal place of business is San Francisco, California, where it is registered as a data broker under California law, and where it maintains the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its marketing, software development, and major policy, financial, and legal decisions.

47. LiveRamp's privacy-invasive conduct as described herein emanated from, and was conceived and executed in, California.

48. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the common law claims of the Class members.

VI. DIVISIONAL ASSIGNMENT

49. Pursuant to Civil L.R. 3-2(c), assignment to this division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this District. LiveRamp's conduct as described below is directed at Internet users and people throughout the United States, including in San Francisco County, California.

VII. STATEMENT OF FACTS

A. LiveRamp Collects, Buys, and Analyzes Vast Amounts of On- and Offline Data to Track Individual Consumers Everywhere on the Internet and in the Real World.

50. LiveRamp, formerly known as Acxiom,[19] is registered as a "data broker" in California (and in other states), which is defined as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.

51. LiveRamp sits at the center of a vast commercial surveillance ecosystem. Its critical function in that ecosystem is to connect (1) *what* third parties know about consumers with (2) the places *where* consumers may be found—both online and in the physical world. "This gives advertisers two critical pieces of information: a person and their intent."[20]

[19] LiveRamp Form 8-K, at 2 (Oct. 1, 2018) https://investors.liveramp.com/static-files/b4a7a41c-288e-4f42-99b6-7fcc1b0701f6 [https://perma.cc/B6HB-YZ7A].

[20] Max Eddy, *How Companies Turn Your Data Into Money*, PC MAG (Oct. 10, 2018),

52. LiveRamp's business is the omnipresent, virtually inescapable tracking of these two data points wherever a person goes in their online *or offline* activity, so that with just one piece of information (a mobile device identifier or email address, for example), LiveRamp can generate a comprehensive identity profile of that person by compiling names, phone numbers, and physical addresses together with online identifiers such as device IDs, cookies, and browsers, thereby creating a "360 degree view" of an individual person.

53. LiveRamp then sells this functionality to a wide range of "partners," allowing them to monitor people as they go about their daily lives, and to communicate with other online actors about those people—most particularly people whom they want to track, profile, advertise, and sell to. As LiveRamp describes its comprehensive consumer profile surveillance services which "[b]uild 360-degree view profiles" of Plaintiffs and Class members:

> Through the process of centralizing data across systems and consolidating consumer profiles, [LiveRamp] offers a comprehensive view of every individual consumer . . . . It enables you to merge identifiers like email addresses and phone numbers with behavioral, demographic, and transactional data to create a unified view of each customer.[21]

54. All of this is done without consumers' consent or even awareness.

55. LiveRamp knows an enormous amount about consumers, but the average consumer knows nothing about LiveRamp. Consumers are therefore unaware of the extent to which the entirety of their online activities are subjected to pervasive, invasive and highly sophisticated tracking, profiling, and targeting as described herein. LiveRamp has accordingly been described as a "Privacy Death Star."[22]

---

https://www.pcmag.com/news/how-companies-turn-your-data-into-money [https://perma.cc/2399-5464].

[21] *What is Data Activation and How Does it Work?*, LIVERAMP (Feb. 13, 2024), https://liveramp.com/blog/what-is-data-activation-and-how-does-it-work/ [https://perma.cc/YJ6N-EAUM].

[22] *See Exposing the Hidden Data Ecosystem of the UK's Most Trusted Charities*, PROPRIVACY (Sept. 10, 2020), https://proprivacy.com/privacy-news/exposing-the-hidden-data-ecosystem-of-the-uks-most-trusted-charities [https://perma.cc/HR44-GZR3] ("Data brokers like Oracle (BlueKai) and LiveRamp (formerly Axicom [*sic*]) have been described as Privacy Death Stars. They probably know more than Google, Facebook, or any other single entity that gathers human-specific trackable intelligence. They are aggregators of data, not just online, but offline too. Everything from credit card transactions to criminal records is gathered from thousands of partners

56. LiveRamp's business revolves around two principal services: "identity resolution" and the "Data Marketplace." As noted above, "identity resolution" refers to the process of merging or "resolving" various distinct data points or "touchpoints" (an email address, a physical address, and a mobile device ID, for example) into a comprehensive identity profile of a single consumer. LiveRamp's principal identity resolution product is the "**RampID,"** a persistent, "omnichannel" identifier created by LiveRamp for individual persons and households.[23]

57. RampIDs are constructed both from **online**[24] data and, through an intermediate identifier called the "AbiliTec ID," **offline**[25] data or "offline PII."[26] This "identity resolution" service allows LiveRamp to identify individuals and to aggregate their many identifiers, which in turn facilitates further synchronizing of personal information with a high degree of confidence. LiveRamp acknowledges that it creates:

> [A] robust identity framework within [its clients] data foundations to provide [them] with an accurate and comprehensive ***360-degree view*** of [their] customers. Our solutions build a single source of truth about the customer, connecting offline and online data sources with a durable, deterministic person-based ID that never fades, even as cookies decay.[27]

---

in order to build detailed dossiers of as many citizens around the world as possible.").

[23] *Identity and Identifier Terms and Concepts*, LIVERAMP, https://docs.liveramp.com/identity/en/identity-and-identifier-terms-and-concepts.html#rampid [https://perma.cc/43XQ-HGFQ]; *Perform Identity Resolution in Snowflake*, LIVERAMP, https://docs.liveramp.com/identity/en/perform-identity-resolution-in-snowflake.html [https://perma.cc/9DXW-HQ75]; *Authenticated Traffic Solution*, LIVERAMP, https://docs.liveramp.com/identity/en/authenticated-traffic-solution.html [https://perma.cc/DS3K-MGN6].

[24] LiveRamp defines the term "online identifiers" as follows: "Usually refers to device identifiers such as cookies and mobile device IDs. These identifiers are also referred to as 'pseudonymous identifiers.'" *See Glossary of All Terms*, LIVERAMP, https://docs.liveramp.com/connect/en/glossary-of-all-terms.html [https://perma.cc/SFV8-3X3H].

[25] LiveRamp defines the term "offline identifiers" as follows: "Usually refers to PII identifiers such as name and postal, email address, and hashed email address. These identifiers are also referred to as 'known identifiers.'" *Id*.

[26] LiveRamp defines "PII" as "Personally identifiable information (such as name and postal, phone number, or email address) which, on its own or when combined with some other data, can be used to identify an individual." *Id*.

[27] *Getting Started with LiveRamp Identity*, LIVERAMP, https://docs.liveramp.com/identity/en/getting-started-with-liveramp-identity.html (emphasis added) [https://perma.cc/L8V8-CA7W].

This conduct—which is largely unknown to the public—violates Plaintiffs' and Class members' reasonable expectation of privacy. As described in the press, "[t]ech companies have repeatedly reassured the public that trackers used to follow smartphone users through apps are anonymous or at least pseudonymous, not directly identifying the person using the phone. But what they don't mention is that an entire overlooked industry exists to purposefully and explicitly shatter that anonymity"—that is the "identity resolution" industry in which LiveRamp is the largest and most significant actor.[28]

58. LiveRamp claims to have "resolved" the identities of more than 250 million consumers in the United States (*i.e.*, virtually every single adult)[29] "and many more worldwide" by assigning them each a unique RampID.[30] LiveRamp can then connect names, postal addresses, email addresses, phone numbers, cookies, mobile device IDs, connected TV device IDs, and custom identifiers or CIDs—all manner of offline and online data—to a RampID.[31] For example, give LiveRamp the device ID of a smart or "connected" TV or any smartphone, and it knows (or claims to know) whom the device belongs to or who is using it.[32] The RampID is thus the equivalent of a permanent and inescapable personal identification number, which allows LiveRamp and its

---

[28] Joseph Cox, *Inside the Industry That Unmasks People at Scale*, VICE (July 14, 2021) https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii [https://perma.cc/D8UB-KXQ5].

[29] As of 2020, the total number of adults in the United States was 258.3 million. *See U.S. Adult Population Grew Faster Than Nation's Total Population from 2010 to 2020*, UNITED STATES CENSUS BUREAU (Aug. 12, 2021), https://www.census.gov/library/stories/2021/08/united-states-adult-population-grew-faster-than-nations-total-population-from-2010-to-2020.html [https://perma.cc/S4PW-4HMG].

[30] *Solutions: Identity Resolution*, LIVERAMP, https://liveramp.uk/identity-resolution/ [https://perma.cc/8PE5-W9VE]; *see also Identity Resolution: What is it and Why is it Important*, LIVERAMP (June 21, 2024), https://liveramp.com/identity-resolution/ [https://perma.cc/244V-BCMB].

[31] *Perform Identity Resolution in Snowflake*, LIVERAMP, https://docs.liveramp.com/identity/en/perform-identity-resolution-in-snowflake.html [https://perma.cc/9DXW-HQ75].

[32] Jeff Chester and Kathryn C. Montgomery, *How TV Watches Us, Commercial Surveillance in the Streaming Era*, CENTER FOR DIGITAL DEMOCRACY, (Oct. 2024), https://democraticmedia.org/reports/how-tv-watches-us-commercial-surveillance-in-the-streaming-era [https://perma.cc/2P3K-JX4L] ("LiveRamp . . . is a major player in the use of CTV data for its "RampID" system. As the company explains, its "people-based IDs" make it possible to 'link individuals and households to the right digital identifiers including cookies, mobile device IDs, Advanced TV IDs, and user accounts at social networks.'").

customers to surveil and manipulate specific individuals, with an incredibly high degree of precision, in perpetuity.

59. LiveRamp's "**Data Marketplace**" provides a platform for hundreds of third-party data brokers to buy and sell vast repositories of detailed consumer information by "segments," or groups of consumers defined by demographic information (quantitative data such as age, gender, or income) or "psychographic" information (qualitative data such as personality traits, attitudes, interests, and values, including religion, political views, and sexual reproductive decisions). LiveRamp, its data "partners," and its customers deploy the consumer information bought on the Data Marketplace to manipulate individual consumers by identifying them through the RampID identity graph system or other identity data wherever they may be found, on- or offline.

60. LiveRamp tracks the lives of the general public in a manner that is opaque, if not invisible, to the people it follows, as they have no direct relationship with LiveRamp.

61. LiveRamp does not even maintain a pretense of having directly obtained the consent of the subjects of its surveillance—*i.e.*, the proposed Classes herein—who have no legal or practical ability to consent to LiveRamp's conduct.

62. LiveRamp reaps great financial benefit from its conduct described herein; LiveRamp generates over half a billion dollars per year trafficking in personal information,[33] and its market capitalization exceeds $2.33 billion.[34]

1. LiveRamp Collects, Buys, and Analyzes Vast Amounts of Offline Data to Construct Real-World Identity Profiles Using Its AbiliTec System.

63. LiveRamp's RampID identity graph system relies on its AbiliTec system, which first assigns individuals an "AbiliTec ID" constructed of real-world "offline" identity information that is

[33] *LiveRamp Announces Fourth Quarter and Fiscal Year Results*, LIVERAMP (May 24, 2023), https://investors.liveramp.com/news-releases/news-release-details/liveramp-announces-fourth-quarter-and-fiscal-year-results [https://perma.cc/GX4Q-F4NN] (2023 Fiscal Year report touts $597 million in total revenue); *LiveRamp Announces Fourth Quarter and Fiscal Year Results*, LIVERAMP (May 22, 2024), https://investors.liveramp.com/news-releases/news-release-details/liveramp-announces-fourth-quarter-and-fiscal-year-results-4 [https://perma.cc/CAA7-SAAS] (2024 Fiscal Year report touts $660 million in total revenue).

[34] LiveRamp Holdings, Inc. (RAMP) Overview, STOCK ANALYSIS, https://stockanalysis.com/stocks/ramp/ [https://perma.cc/9BUH-XPM3].

then used to link their online activity with a RampID. AbiliTec links different offline identifiers (*e.g.*, email address, name, and postal address) to each other, allowing LiveRamp's clients to "resolve" this information "into a unified view of those consumers."[35] AbiliTec combines "[c]ommon matching techniques"—such as "probabilistic matching, approximate string matching, and other typical matching approaches, such as edit distance routines to provide matches across names and addresses present within a client's data"—with "comparison of customer data to a vast multi-sourced historical repository of consumer contact information"[36] to identify individual consumers and assign them each a single AbiliTec ID.

64. AbiliTec IDs are purportedly constructed from "a vast, multi-sourced historical identity graph containing over 40 years of consumer contact information from over 150 data sources, including over 4.5 billion name and postal records, over 1.1 billion email addresses, and over 600 million phone numbers."[37] AbiliTec's "knowledge bases are sourced from hundreds of contributors and contain multiple name, address, and email representations for individuals, as well as the associative data to resolve the data points to an individual over time."[38] "[S]ources included in the knowledge bases include . . . public record data[,] publically [sic] available data[, and] self-reported information."[39] "LiveRamp purchases its email-to-postal address match data from various third-party providers."[40]

---

[35] *Offline Identity Resolution with AbiliTec*, LIVERAMP, https://docs.liveramp.com/identity/en/offline-identity-resolution-with-AbiliTec.html [https://perma.cc/TY85-52C4].

[36] *Understanding AbiliTec*, LIVERAMP, https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [https://perma.cc/C7ND-Z6XE].

[37] *The AbiliTec Identity Graph*, LIVERAMP, https://developers.liveramp.com/abilitec-api/docs/the-abilitec-identity-graph-1 [https://perma.cc/L49H-9PEN].

[38] *RampID Methodology*, LIVERAMP, https://docs.liveramp.com/identity/en/rampid-methodology.html#idm46463362786624 [https://perma.cc/8WFU-C2JA].

[39] *Id.*; LiveRamp, Form 10-K (Mar. 31, 2021), https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [https://perma.cc/KFM8-8KWQ].

[40] *LiveRamp Match Data Sources*, LIVERAMP, https://docs.liveramp.com/connect/en/liveramp-match-data-sources.html [https://perma.cc/W7DC-5FTW].

65. In addition to collecting and processing this extensive offline information about individual consumers, LiveRamp's AbiliTec system also collects and processes "[c]onsumer associative data, such as gender or year of birth (used to build people and household formations)"; and "[i]nternal metadata, such as frequencies, classifications, and thresholds for making linking decisions."[41]

66. When LiveRamp's clients send a piece of identifying information—such as a name, postal address, email address or phone number—to LiveRamp, the AbiliTec system matches this information to existing records and returns one or several AbiliTec IDs referring to an individual consumer, a household, or a place/address. LiveRamp can then use these identifiers to join or match scattered and fragmented personal information collected from a variety of different sources into a single customer record.

67. The AbiliTec ID technology follows people across time and space as they change names (due to marriage, divorce, gender transition, or for other reasons) and residences. As LiveRamp says, "people are dynamic: they move houses, change jobs, switch phones, share computers, and upgrade their tech. In the U.S., in 2018 alone, there were 36 M residential moves, 4 M births, 2.2 M marriages, and almost 800 K divorces."[42] LiveRamp's AbiliTec system exists precisely to *overcome* this human dynamism through pervasive data collection and tracking. Over time, each of these events builds a more complete picture of that person's identity.

68. LiveRamp zealously describes the scope of its surveillance, touting its ability to connect real-world people instantaneously and persistently with both offline and online identifiers, "with a high degree of speed and accuracy":

> Our proprietary, patented recognition technology draws upon an extensive historical reference base to identify and link together multiple consumer records and identifiers. We use the pioneering algorithms of AbiliTec® and deterministic digital matching to link individuals and households to the right digital identifiers including

[41] *Understanding AbiliTec*, LIVERAMP, https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [https://perma.cc/C7ND-Z6XE].

[42] *File Output Options for Measurement Enablement Workflows*, LIVERAMP, https://docs.liveramp.com/safe-haven/en/file-output-options-for-measurement-enablement-workflows.html#why-records-might-have-multiple-rampids-70-19340 [https://perma.cc/99SY-X4C3].

> cookies, mobile device IDs, Advanced TV IDs, and user accounts at social networks. As a result, we are able to match online and offline data with a high degree of speed and accuracy.[43]

2. LiveRamp Collects, Buys, and Analyzes Vast Amounts of Online Data to Track Real-World Consumers' Digital Activities Using the RampID Identity Graph System.

69. LiveRamp's RampID identity graph system builds on its AbiliTec ID system, by expanding the scope of identifying information gathered and processed by LiveRamp into the digital space, allowing its clients to connect individual consumers' offline personal information with their online activities. LiveRamp refers to its AbiliTec system as an "offline identity graph," and to its RampID system as its "online identity graph."[44]

70. The first step in the construction of a "maintained" RampID—or a RampID "representing an individual that LiveRamp fully recognizes" and can match to a complete set of that individual's personal information[45]—is to assign a "derived" RampID to a single personal information "touchpoint": an email address, for example.[46] The touchpoint(s) are then associated with as many other "offline" personal information touchpoints as possible using its AbiliTec system.[47] Once sufficient touchpoints have been associated with one another a sufficient number of times, LiveRamp will merge the disparately derived RampIDs attached to each piece of personal information into one "maintained" RampID, to whom all these pieces of information (are thought to) belong.[48] In this way, LiveRamp creates the equivalent of a permanent "Internet Social Security Number" that is accurately and inescapably associated with virtually every adult in the United States.

---

[43] LiveRamp, Form 10-K (Mar. 31, 2021), https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [https://perma.cc/KFM8-8KWQ].

[44] *LiveRamp Data Security Overview*, LIVERAMP, https://docs.liveramp.com/connect/en/liveramp-data-security-overview.html [https://perma.cc/V8C5-PH5Q].

[45] *Interpreting RampID, LiveRamp's People-Based Identifier*, LIVERAMP, https://docs.liveramp.com/identity/en/interpreting-rampid,-liveramp-s-people-based-identifier.html#idm46463362751232 [https://perma.cc/B2BE-4L8S].

[46] *Id.*; *Touchpoints*, LIVERAMP, https://docs.liveramp.com/connect/en/touchpoints.html [https://perma.cc/D6BT-ABHP].

[47] *RampID Methodology*, LIVERAMP, https://docs.liveramp.com/identity/en/rampid-methodology.html#idm46463362804192 [https://perma.cc/6NK4-RGFY].

[48] *Interpreting RampID, LiveRamp's People-Based Identifier*, LIVERAMP,

71. The RampIDs are then, with the help of data provided by a large network of "partners," connected to various online identifiers such as "partner-specific cookies, mobile IDs, and other online IDs."[49] The list of online identifiers LiveRamp admits to maintaining on one consumer stretches ten pages, including custom IDs, cookie IDs, and mobile device IDs as well as the census block groups the IDs are typically located in, IP addresses, connected TV IDs, browser used, ISP used, brand properties visited, estimated minimum visit durations at these properties, and dimensions of the user's screen that can be used in connection with other data to uniquely fingerprint the user.[50] The scale of LiveRamp's surveillance is staggering. Indeed, immediately after the spinoff from Acxiom in 2018, LiveRamp's CEO was explicit that LiveRamp's business model is to place every person in the world under constant surveillance by connecting every person's identity to all available information about them, from any source: "What LiveRamp has done is, they've gone and integrated *all* of the world's data providers, linked that data to *all* of the world's people, and then in turn, link that to buil[d] connections to *all* of the world's use cases."[51]

72. Just as LiveRamp's AbiliTec system depends on the collection of vast amounts of *offline* personal information, the operation of LiveRamp's RampID identity graph system depends on the collection of vast amounts of *online* personal information about as many people as possible. LiveRamp uses multiple means to collect and process this data, including its own suite of internet technologies, as well as from its acquisition of data from its "partners," as described below.

73. Cookies. As web browsers do not provide their own unique identifiers that consistently refer to their users, data brokers like LiveRamp use "cookies" or other similar browser storage mechanisms like "localStorage"[52] to create unique online personal identifiers, or "cookie

---

https://docs.liveramp.com/identity/en/interpreting-rampid,-liveramp-s-people-based-identifier.html#idm46463362751232 [https://perma.cc/B2BE-4L8S].

[49] *Getting Started with Activation*, LIVERAMP, https://docs.liveramp.com/connect/en/onboarding-your-data.html#overall-onboarding-steps [https://perma.cc/NS52-GCUC].

[50] *See* Data Subject Access Request Explanatory Information Document Consumer Data at 8, version 3.2, LIVERAMP (May 31, 2024).

[51] Robert Andrews, *After IPG Sale, Acxiom's LiveRamp is Now 'Neutral': CEO Howe*, BEET.TV (OCT. 1, 2018), https://www.beet.tv/2018/10/acxiom-scott-howe.html (emphasis added).

[52] *Other Use Cases for Retrieving Envelopes*, LIVERAMP, https://docs.liveramp.com/privacy-manager/en/other-use-cases-for-retrieving-envelopes.html [https://perma.cc/JV2C-V546].

IDs," for the users of browsers. Many websites embed software from third-party companies that store cookie IDs in the user's browser, which they can retrieve during subsequent visits to these websites. As such, third-party companies can recognize website visitors when they return to these websites at a later point in time.

74. When third-party companies want to exchange personal information about the behaviors or characteristics of website visitors among each other, they must ensure they are referencing the same users. For this purpose, they map cookie IDs maintained by one third-party company to cookie IDs maintained by another third-party company. This process, which involves the exchange of cookie IDs between these third-party companies, is often referred to as "cookie syncing" or "ID syncing." As a result, third-party companies can persistently identify users of web browsers and thus recognize, track, follow, profile, and target people across companies and websites.

75. LiveRamp deploys its own proprietary cookies across numerous websites, and it also collects cookie IDs from "400+" other companies,[53] including Google, Facebook, Amazon, Microsoft, Salesforce, Oracle, Neustar, Nielsen, The Trade Desk, and Quantcast.[54] LiveRamp can then synchronize all of those cookie IDs to match a particular cookie ID not only to "other partner cookies," but also to "mobile devices, proprietary platform IDs, and RampIDs."[55] This cookie syncing process involves the constant exchange of personal information across many companies at a massive scale.

76. Web Match Tags. LiveRamp's "Web Match Tags" allow it to establish links between consumers' email addresses and cookie IDs. LiveRamp's "match partners," who are part of its "match network," add LiveRamp's Web Match Tag "to all website pages where a user's email

[53] *How LiveRamp Addresses Fragmented People-Based Links*, LIVERAMP, https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [https://perma.cc/S4HA-645P].

[54] *Request a Reach Estimate*, LIVERAMP, https://docs.liveramp.com/safe-haven/en/request-a-reach-estimate.html [https://perma.cc/2QHK-2B95]; *Match, OIDL & ATS Partners*, LIVERAMP, https://web.archive.org/web/20220523082051/https://liveramp.fr/partenaires/ [https://perma.cc/VP59-YCH4].

[55] *Identity Translation*, LIVERAMP, https://docs.liveramp.com/identity/en/identity-translation.html [https://perma.cc/9BLU-KT97].

addresses can be populated," for example, on "post-registration pages," "post-login pages," "returning-user pages" and "landing page(s) associated with any links in your email newsletters."[56] As soon as a match partner has access to a user's email address—for example, because the user just registered an account—the Web Match Tag sends the hashed email address, *i.e.*, sends an email identifier derived from the user's email address, and LiveRamp's cookie ID to LiveRamp. LiveRamp can then create a new link between an email address and a cookie ID in its identity graph. LiveRamp uses similar technologies to create links between email addresses and mobile device IDs,[57] and between email addresses and custom IDs[58] (which are "account-based" user IDs "assigned to users by a specific platform, such as Google or Facebook").[59]

77. Client-Side Tags. LiveRamp deploys "Client-Side Tags" and "Enhanced Client-Side Tags" on websites to gather data on consumers' online activities. LiveRamp's Client-Side Tags are deployed via "tracking pixels"—surreptitious online tracking mechanisms, sometimes also called "spy pixels"[60]—and automatically "capture," or intercept, the URLs of the web pages visited, the exact date and time of the visit, and a variety of other information such as "page views," "ad views, adding items to cart, or completing a transaction."[61] This captured data then goes through LiveRamp's recognition process to match the website visitors to their specific RampIDs.

---

[56] *For Match Partners: Implementing LiveRamps's Web Match Tag*, LIVERAMP, https://docs.liveramp.com/connect/en/for-match-partners--implementing-liveramp-s-web-match-tag.html [https://perma.cc/KE48-6JTW].

[57] *For Match Partners: Uploading Mobile App Files*, LIVERAMP, https://docs.liveramp.com/connect/en/for-match-partners--uploading-mobile-app-files.html [https://perma.cc/KE48-6JTW].

[58] *Website Data Monetization Through Customer ID Matching*, LIVERAMP, https://docs.liveramp.com/connect/en/website-data-monetization-through-customer-id-matching.html [https://perma.cc/9RLV-UWCZ].

[59] *Identity and Identifier Terms and Concepts*, LIVERAMP, https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [https://perma.cc/43XQ-HGFQ].

[60] WIKIPEDIA, *Spy Pixel*, https://en.wikipedia.org/wiki/Spy_pixel [https://perma.cc/3XE7-QXKZ].

[61] *LiveRamp's Client-Side Tags*, LIVERAMP, https://docs.liveramp.com/identity/en/implementing-liveramp-s-client-side-tag.html [https://perma.cc/C79J-5BXD]; *Implementation Methods for Client-Side Tags*, LIVERAMP, https://docs.liveramp.com/identity/en/implementation-methods-for-client-side-tags.html [https://perma.cc/S9CC-SEZ4]; *Data Automatically Captured for Client-Side Tags*, LIVERAMP, https://docs.liveramp.com/identity/en/data-automatically-captured-for-client-side-tags.html [https://perma.cc/LA5R-FPDA]; *Placing Client-Side Tags in*

78. Authenticated Traffic Solutions (ATS) JavaScript Code and Software Development Kit (SDK). LiveRamp's "ATS.js" JavaScript Code, implemented through its Enhanced Client-Side Tags, intercepts personal information, such as email addresses and phone numbers, communicated by Class members to websites, and uses that information to create a universal identifier that is unambiguously linked to a specific person for targeting and manipulation by LiveRamp's clients. The ATS.js JavaScript code uses so-called "event listeners" to detect specific types of contents of communications from class members to websites and intercept those contents and simultaneously transmit them to LiveRamp. "Event listeners" are portions of the JavaScript code that "listen" for certain input actions by the internet user—such as "mouse clicks, keyboard presses, and scrolling," and record them in specific ways.[62] Specifically, once ATS.js has been deployed on a website or in an app, ATS.js listens for and intercepts email addresses and phone numbers communicated to that website or app. LiveRamp's "ATS Mobile SDK" (or Software Development Kit) includes largely identical functionality that is deployed on mobile devices.

79. In sum, at the end of the "identity resolution" process, by using the RampID identity graph system, LiveRamp can take any item of real-world personal information (postal address, for example) and link that item to any number of online identifiers (Facebook IDs, for example) across the Internet. This allows thousands of companies to send names, postal addresses, or email addresses

Advertisements, LIVERAMP, *https*://docs.liveramp.com/identity/en/placing-client-side-tags-in-advertisements.html [https://perma.cc/8JZH-TQ8D].

[62] *Event Listeners in JavaScript: The Ultimate Guide*, COD;NN, https://www.codinn.dev/javascript/event-listeners [https://perma.cc/5MTQ-43AF].

to LiveRamp, receive the corresponding RampIDs, and then match them with online identifiers that are also linked to RampIDs from many other companies, as shown in the image below:[63]

80. As people move from one website, mobile app, or other digital product or service to the next (potentially using different emails, passwords, usernames, and devices to do so), they reasonably expect activity in one digital "silo" to be kept in that silo. Plaintiffs and Class members have no expectation that companies like LiveRamp sit behind those identifiers diligently and constantly working to match them to real-world personal information and "resolve" them to individual persons.

81. As explained below, LiveRamp monetizes this mass surveillance and tracking by means of "Data Onboarding," LiveRamp's "Authenticated Traffic Solution," the Data Marketplace, and related services.

[63] Illustration of AbiliTec ID/Ramp ID System. LiveRamp Presentation, *The Future of Addressability*, at 10, (2022), https://files.ctctusercontent.com/75d73837001/e8858146-a9f4-4518-9bc1-b355b98065f3.pdf [https://perma.cc/4MF7-LC4E].

B. Through "Data Onboarding," and Identity Resolution, LiveRamp and Its Customers Target Class Members Wherever They Are in the Digital and Physical Worlds.

82. "Data onboarding" or "Activation" is "the process of connecting your customer data to the digital marketing applications and media platforms that you work with."[64] For example, consider a business with a customer file (often called a "CRM" or customer relationship management information) it wishes to use to target digital advertising to its customers outside its (digital or physical) property. The business's customer files contains its customers' personal information, such as names and email addresses, as well as segment data (or "group[s] of your records that are defined by a specific attribute"),[65] such as gender. The business uploads its customer file to LiveRamp and specifies a desired platform or "destination" for its advertising, such as Facebook.

83. LiveRamp, through its identity resolution services, matches this personal information to a RampID. The customers' RampIDs are then matched to destination-specific identifiers such as cookies, mobile IDs, and custom IDs or "CIDs" such as, in this example, FacebookIDs, using LiveRamp's online Match Network. LiveRamp delivers the customer file (whose personal information has now been translated into destination-specific identifiers) to the destination, where the business uses its delivered segments to target advertising through the tools and UI provided by the destination. LiveRamp counts more than 500 advertiser destinations, which it collects in a public directory,[66] and offers to add more "on request."[67]

---

[64] *Activation Intro Video Series*, LIVERAMP (first video, start at 00:35 seconds), https://docs.liveramp.com/connect/en/activation-intro-video-series.html [https://perma.cc/82XC-CQ3P].

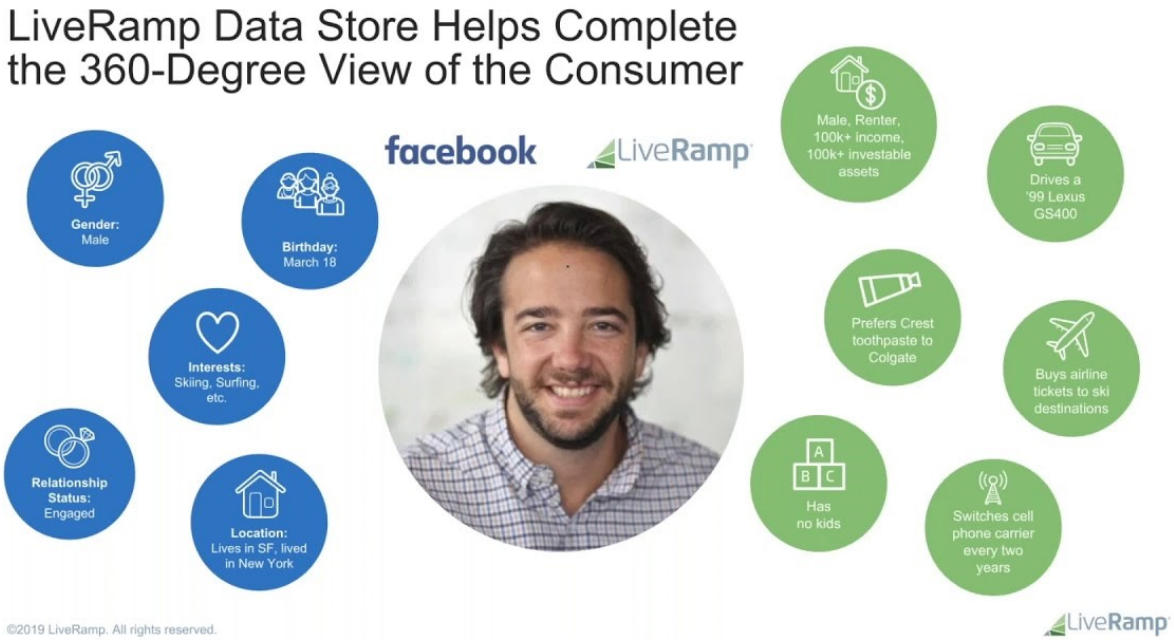
[65] *Activation Terms and Concepts*, LIVERAMP, https://docs.liveramp.com/connect/en/activation-terms-and-concepts.html [https://perma.cc/XJ8C-RV7M].

[66] *LiveRamp Partner Ecosystem*, LIVERAMP, https://partner-directory.liveramp.com/ [https://perma.cc/E4CC-UXY2].

[67] *Getting Started with Activation*, LIVERAMP, https://docs.liveramp.com/connect/en/onboarding-your-data.html#overall-onboarding-steps [https://perma.cc/NS52-GCUC].

84. LiveRamp has 825 direct clients and thousands of indirect ones. Most are large players in the data and AdTech industry, who themselves process personal information on behalf of "myriad web and app publishers, advertisers and other businesses."[68]

85. LiveRamp is ubiquitous on the web and operates in tandem with the largest internet technology companies involved in surveilling and extracting data from internet users. For example, one study found that 96 percent of Facebook users had information about them shared by LiveRamp with Facebook.[69] LiveRamp markets its ability to share data and combine data with Facebook to "complete the 360-degree view of the consumer"—including minute details such as whether the person is married or engaged, whether they are a renter, whether they make more than $100,000 a year, the year and make of the car they drive, whether they have children, and even their preferred brand of toothpaste—via the following graphic:[70]



[68] Wolfie Christl and Alan Toner, *Pervasive identify surveillance for marketing purposes*, CRACKED LABS (Feb. 2024), https://crackedlabs.org/dl/CrackedLabs_IdentitySurveillance_LiveRamp.pdf [https://perma.cc/E4C6-27BA].

[69] Jon Keegan, *Each Facebook User is Monitored by Thousands of Companies*, THE MARKUP (June 8, 2023) https://themarkup.org/privacy/2024/01/17/each-facebook-user-is-monitored-by-thousands-of-companies-study-indicates [https://perma.cc/S66F-M5AT].

[70] LiveRamp, *Using Third-Party Data With Facebook Campaigns | LiveRamp*, YOUTUBE (Feb. 26, 2020), https://www.youtube.com/watch?v=ik1SgiNdRu0 [https://perma.cc/D99S-SBVS].

86. Data onboarding and identity resolution allows LiveRamp and its clients to conduct a covert but omnipresent campaign against consumers' agency and autonomy by saturating their immediate digital and even physical environments in targeted, tailored messages—without consumers even knowing this is happening. For example, one LiveRamp brochure[71] offers the following examples of "sweet" use cases for identity resolution, facilitated through data onboarding:

- A cable TV network tying viewers to car lease expiration dates, to allow ad buyers to target individual viewers whose leases are soon expiring with car ads.
- A retailer tracking which emails from *other* retailers prospective customers open, and using the results to target prospective customers through their own emails as well as tracking in-store sales.
- A retailer targeting "high value" shoppers with *physical digital billboards* based on their location data; in other words, showing ads on a physical billboard that are tailored and targeted to one specific person based on that person's proximity to the billboard.
- A retailer using in-store electronic "beacons" to determine when their customers were browsing in the store and serve them targeted advertising based on their real-time physical locations within the stores.[72]

87. These examples, drawn from LiveRamp's own marketing materials, vividly illustrate LiveRamp's endeavor to remove all digital and physical boundaries separating its clients from Class members, and describes the extent to which LiveRamp openly advertises its ability to facilitate the tracking of every aspect of a consumer's online and offline activities, including tracking their web browsing activity, TV viewing habits, real-time physical location, and in-store purchases.

C. Through "Authenticated Traffic Solutions" or "ATS," LiveRamp Enables Privacy-Invasive "Real-Time Bidding" Based on Class Members' Real-World Identities.

88. LiveRamp's "Authenticated Traffic Solutions" or "ATS" business—based on the ATS.js JavaScript mechanism described above—likewise monetizes the RampID identity profiles

[71] *13 Sweet Identity Resolution Use Cases*, LIVERAMP, https://lp.liveramp.com/rs/320-CHP-056/images/LiveRamp%20UK%20-%2013%20Sweet%20identity%20resolution%20use%20cases.pdf [https://perma.cc/K76Q-D3U7].

[72] LiveRamp, *IdeaBook 300 Ways To Do People-Based-Marketing*, https://02f0a56ef46d93f03c90-22ac5f107621879d5667e0d7ed595bdb.ssl.cf2.rackcdn.com/sites/10980/uploads/23548/ideabook-201820180528-1031-xtba2a.pdf [https://perma.cc/MNY4-G26Y].

by allowing LiveRamp clients to deploy them against consumers wherever they may be at the moment.

89. ATS functions by converting the email addresses and phone numbers Class members use to log in to websites into RampIDs connected to LiveRamp's identity profiles. When a user provides "their identifier on your website" (an email address, for example), "ATS obtains the configuration and transforms it into an encrypted identity envelope containing LiveRamp's pseudonymous identifier, RampID."[73] That RampID can then be used to identify that Class member and target them in real time through the "Real-Time Bidding" advertising ecosystem.[74]

90. Real-Time Bidding is the instantaneous auction system which underlies a significant amount of online advertising. It is widely viewed as privacy invasive:

> What is Real Time Bidding? It's the biggest illegal data breach ever recorded, for a start. The private things you do and watch online are collected from a vast system that operates behind the scenes on virtually every website and app. This allows 'data broker' companies to collate your data – including your sexuality, your medical conditions, your location – to form highly sensitive personal profiles about you. The data breach occurs in online advertising's Real-Time Bidding (RTB) system, hundreds of billions of times daily. This is the biggest data breach the world has ever seen.[75]

91. In other words, ATS allows publishers, advertisers, and other companies involved in Real-Time Bidding to utilize the real-world identities of internet users—based on their own email addresses—and track and manipulate them accordingly. Once these email addresses and phone numbers have been intercepted, they are used to associate that web browsing instance with the identity profile it maintains on that person. That profile is then made available to third parties

[73] *Authenticated Traffic Solution*, LIVERAMP, https://docs.liveramp.com/connect/en/authenticated-traffic-solution.html [https://perma.cc/A9ED-55WE].

[74] *See What is Real Time Bidding?*, IRISH COUNSEL FOR CIVIL LIBERTIES, https://www.iccl.ie/what-is-real-time-bidding/ [https://perma.cc/MRY5-95F4].

[75] *Id.*

through the Real-Time Bidding advertising ecosystem.[76] This enables many different actors "across the open web to know that they are "talking" about the same persons.[77]

92. Plaintiffs and Class members do not, by virtue of simply signing in to online services that they use throughout the course of their daily lives, consent to the creation of an unavoidable and permanent internet identification number that follows them throughout their lives and that can be used by commercial or political actors to surveil and manipulate them.

D. Through Its Data Marketplace, LiveRamp Facilitates the Sale of Vast Amounts of Sensitive Personal Information About Consumers and Facilitates the Construction of Detailed Consumer Profiles.

93. LiveRamp's identity profiles and their uses as described above, standing alone, violate Plaintiffs' privacy rights. However, LiveRamp further invades Plaintiffs' privacy through the purchase and sale of highly detailed personal information about Plaintiffs and Class members on its Data Marketplace.

94. LiveRamp's Data Marketplace is an online market trading in the sensitive and private personal information of hundreds of millions of people. LiveRamp describes this massive, international personal information bazaar as making available to participants "multi-sourced insight into approximately 700 million consumers worldwide."[78]

95. LiveRamp's Data Marketplace "allows data buyers to gain access to third-party data from over 160 top data sellers, each offering a wide range of segment types, including behavioral, geographic, demographic, and more."[79] LiveRamp's Data Marketplace vendors are collected in a public directory.[80]

---

[76] Wolfie Christl and Alan Toner, *Pervasive identity surveillance for marketing purposes*, at 53 CRACKED LABS (Feb. 2024), https://crackedlabs.org/dl/CrackedLabs_IdentitySurveillance_LiveRamp.pdf [https://perma.cc/E4C6-27BA].

[77] *Id.*

[78] LiveRamp, Form 10-K (Mar. 31, 2021), https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [https://perma.cc/KFM8-8KWQ].

[79] *Getting Started with Data Buying*, LIVERAMP, https://docs.liveramp.com/connect/en/getting-started-with-data-buying.html [https://perma.cc/H48Y-WS7J].

[80] LiveRamp, *Data Marketplace Data Provider Directory*, (May 2023),

96. As recently reported, LiveRamp's clients bought and sold "segments" of digital identifiers associated with people with cancer, union members, Muslims, Jewish people, African Americans, poor people, payday loan prospects, online gamblers, unemployed individuals who were "seen at clinics/hospitals" and users of the LGBT dating app Grindr.[81]

97. LiveRamp's Data Marketplace is filled with segments containing highly intimate, sensitive, and intrusive information about Plaintiffs and Class Members. For example, the following segments are or were available through the LiveRamp Data Marketplace:

a. Examples of Medical Segments:

- Quotient Technology > Family Planning > Male/female Contraceptive > Condom > Church & Dwight Condom Buyer (Row 564673)[82]
- Clickagy > Health > Addictions > Drugs (Row 356609)
- Clickagy > Health > Addictions > Sex (Row 219275)
- Clickagy > Partners > Engine Group > Healthcare/Lifestyle > Cancer Sufferers/Information Seekers (Row 460467)
- Clickagy > Demographics > Presence of Children > Pregnant (Prenatal) (Row 219146)
- Audience Now by Fluent > Health > Visit Doctor Often (Row 411150)
- Lifescript > Declared Health Interest > Urinary & Bowel (Row 121858)
- Kantar > US > Health and Wellness > Conditions and Treatments > Fibromyalgia (Row 510394)

b. Examples of Financial Segments:

- NinthDecimal > Amnet > BlueCross > People seen at Clinics/Hospitals who are Unemployed – Precise (Row 217353)
- TransUnion > Consumer Finance > Credit Behavior > Target by Transactor or Revolver Card Behavior > Average Consumer Doesnt

---

https://view.highspot.com/viewer/6466ab9408ad6e9290593413 [https://perma.cc/A93G-GWCA].

[81] Jon Keegan and Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you [https://perma.cc/MUG2-N38J]. The Xandr spreadsheet file is available at: https://web.archive.org/web/20230525225541mp_/https://xandr-be-prod.zoominsoftware.io/bundle/monetize_monetize-standard/page/attachments/data-marketplace-buyer-overview/data_marketplace_public_segments_pricing_05212021.xlsx.

[82] Row citations are to the Xandr spreadsheet file, *supra.*

Pay the Full Balance on One or More Credit Cards (Revolver Behavior) (Row 189081)

- Powerlytics Stirista Fusion > Income Changes > Household Income 3 Year Percent Change > Household Income Decrease 20-25% in the Last 3 Years (Row 572156)
- Stirista > Consumer > White-Collar Working Class > Low Income (Row 136175)
- Datastream Group > Payday Flag > Consumer has Requested a Payday Loan (Row 134280)
- Cross Pixel > Audience portraits > Finance > Low Credit Scores (Row 363466)
- Clickagy > Partners > Engine Group > Sociodemographics > Gamblers (Row 460474)
- Audience Now by Fluent > Health > Health Insurance > Uninsured (Row 367564)

c. Examples of Race/Ethnicity Segments:

- Stirista > Consumer > Race > African-American (Row 364042)
- PlaceIQ > Demographic > Race > Hispanic (Row 445612)
- Stirista > Voter > Ethnicity > Bosnian Muslim (Row 159730)

d. Examples of Political Segments:

- Infogroup > B2C > Politics > Voter Segment > Gen X > Conservative Voters – Co-op Sourced (Row 132803)
- L2 Voter Data > Lifestyle & Issue Data > HaystaqDNA > Abortion > Pro > Choice (Row 557936)
- Infogroup > Consumer > US Politics > Issues & Advocacy > Muslim Ban – Support (Row 518244)
- Alliant > Interest Propensities > Issues & Causes > Gun Rights (Row 373412)
- Infogroup > B2C > Politics > Issues > Domestic > Same-Sex Marriage > Opponents – Co-op Sourced (Row 160249)
- Infogroup > B2C > Politics > Issues > Social > Transgender Bathroom Rights > Opponents – Co-op Sourced (Row 154522)

e. Examples of Personal/Family Segments:

- Lifescript > Declared Family > Parents of Teenagers (Row 121831)
- Lifescript > Declared Family > New Moms_07 (Row 122994)
- PushSpring > Custom > Xaxis LA > Xaxis LA: Nature Made: Pregnancy Location and Action - Cross Device (Row 538932)

- Twine > Mobile Apps > Top Mobile Apps > Grindr - Gay chat (Row 349938)

f. Examples of Religion-Based Segments:

- Infogroup > Consumer > US Politics > Demographics > Religion > Jewish (Row 518048)
- American Student Marketing > Religious Affiliation > Islam/Muslim (Row 164263)
- Infogroup > Consumer > US Politics > Demographics > Religion > Protestant (Row 518142)
- Infogroup > Consumer > US Politics > Issues & Advocacy > Religion--Attends Church Frequently (Row 518144)
- Infogroup > Consumer > US Politics > Demographics > Religion > Catholic (Row 518248)
- 180byTWO > Mobile > B2C > Religion > Sikh (Row 135185)

98. The Data Marketplace allows sellers to sell data on Class members with apparently minimal review that consists only of an unspecified "privacy review and approval" which "usually takes 1-2 days."[83]

99. LiveRamp claims to prohibit putting certain sensitive segment data up for sale on the Marketplace,[84] but it is impossible to tell whether and how LiveRamp enforces these restrictions. For example, the policy claims to prohibit segments "relating to" "reproductive health and rights, pregnancy, and fertility,"[85] but in reality vast amounts of records are for sale on the Marketplace that target pregnancy and interest in pregnancy.[86] LiveRamp's publicly-available technical documentation blurs out any information about the segments actually being bought and sold on the Marketplace, making it impossible for Plaintiffs to directly assess the full scope of data available.[87]

---

[83] *Getting Started with Data Selling*, LIVERAMP, https://docs.liveramp.com/connect/en/getting-started-with-data-selling.html [https://perma.cc/8LCH-KY34].

[84] *LiveRamp's Data Marketplace Data Policy*, LIVERAMP, https://docs.liveramp.com/connect/en/liveramp-s-data-marketplace-data-policy.html [https://perma.cc/VQZ7-6B3B].

[85] *Id.*

[86] Shoshana Wodinsky and Kyle Barr, *These Companies Know When You're Pregnant—And They're Not Keeping It Secret*, GIZMODO (July 30, 2022), https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426 [https://perma.cc/FYW2-UL7B].

[87] *See, e.g.*, *Buying Segment Data from the Data Marketplace*, LIVERAMP,

100. Notably, even within LiveRamp's own marketing materials, Data Marketplace vendors advertise the sale of sensitive data that LiveRamp claims to prohibit. For example, Fyllo, "the world's largest ecosystem of cannabis and CBD purchase data," makes available for sale on LiveRamp's Data Marketplace "millions of consumer profiles across hundreds of traditional categories [s]ourced from offline, PII-based cannabis- and CBD transaction data."[88] This is despite LiveRamp's supposed prohibition on the sale of segments targeting marijuana or THC users.[89]

101. The more than 160 data brokers doing business on the Marketplace[90] themselves may aggregate their data from dozens or hundreds of other sources, and the scope of their reach can be staggering. One of the best known, TransUnion, offers datasets drawn from "34 million unique businesses from over 120 public and private data sources linked to individuals," including "[c]onsumer finance audiences . . . anchored in offline financial and insurance information."[91] Credit reporting agency Experian offers for sale "[t]housands of attributes on more than 300 million consumers and 126 million households . . . from various sources including public records, census data, purchase/transactional data, etc."[92]

102. In June 2023, The Markup, a nonprofit digital newsroom focused on technology and privacy, analyzed a spreadsheet of 650,000 audience segments found on the website of Microsoft's

---

https://docs.liveramp.com/connect/en/buying-segment-data-from-the-data-marketplace.html [https://perma.cc/F3AL-JA58].

[88] LiveRamp, *Data Marketplace Data Provider Directory*, at slide 83 (May 2023), https://view.highspot.com/viewer/6466ab9408ad6e9290593413 [https://perma.cc/A93G-GWCA].

[89] *LiveRamp's Data Marketplace Data Policy*, LIVERAMP, https://docs.liveramp.com/connect/en/liveramp-s-data-marketplace-data-policy.html [https://perma.cc/VQZ7-6B3B].

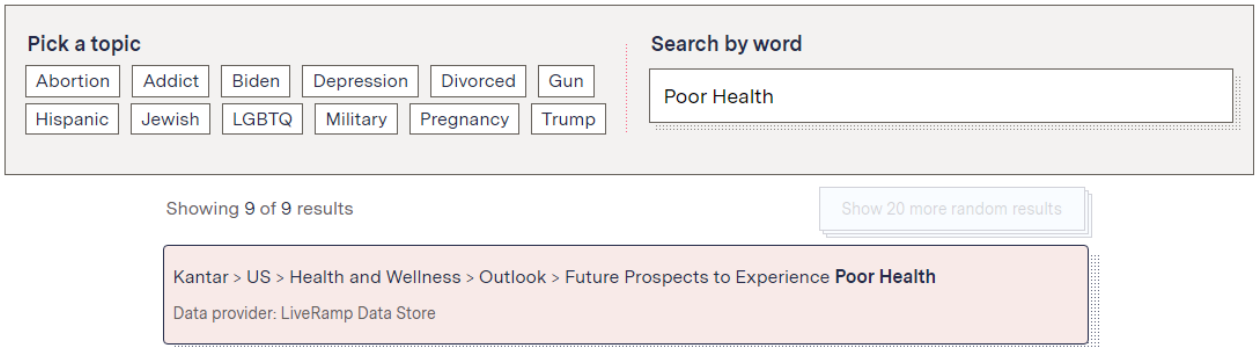
[90] *Getting Started with Data Buying*, LIVERAMP, https://docs.liveramp.com/connect/en/getting-started-with-data-buying.html [https://perma.cc/H48Y-WS7J].

[91] LiveRamp, *Data Marketplace Data Provider Directory*, at slide 181 (May 2023), https://view.highspot.com/viewer/6466ab9408ad6e9290593413 [https://perma.cc/A93G-GWCA].

[92] LiveRamp, *Data Marketplace Data Provider Directory*, at slide 72 (May 2023), https://view.highspot.com/viewer/6466ab9408ad6e9290593413 [https://perma.cc/A93G-GWCA].

ad platform Xandr.[93] Of these, 12.6 percent, or more than 78,000, apparently originated on LiveRamp's Data Marketplace.[94]

103. Searching the spreadsheet illustrates the vast amount of sensitive consumer data being bought and sold on the LiveRamp Data Marketplace and the detailed profiles on Plaintiffs and Class members that can be constructed using it. For example, 159 segments relate to "Trump;" of these, LiveRamp sells segments titled, for example, "Trump – Views by Republican Leaning Voters - Oppose Both Policies and Man," "Distrust Trump Media Coverage," and "Trump-Concerned About His Potential Business Conflicts – No."[95] Twelve segments relate to transgender issues; of these, three were sold on the Marketplace, including "Allow Transgender Bathroom - Oppose" and "Allow Transgender Bathroom - Support."[96] LiveRamp sells segments titled "Use Any Rx Treatment for Depression," "Credit Crunched - City Singles," and "Future Prospects to Experience Poor Health."



104. LiveRamp's technical materials explain to its clients how to whitewash the segments they make available for sale in order to conceal the sensitive nature of the information they are selling. For example, LiveRamp advises that instead of (accurately) describing a sensitive segment

[93] Jon Keegan and Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you [https://perma.cc/MUG2-N38J].

[94] *Id.*

[95] *Id.*

[96] *Id.*

as containing "consumers who are **barely scraping by** and are **always borrowing money** from friends and family," Data Marketplace data sellers should instead describe their segment as containing "consumer [*sic*] who are **likely to borrow money**."[97]

105. Similarly, while LiveRamp purports to prohibit segments regarding "Cannabis/marijuana (THC, not CBD)," LiveRamp also states—via the equivalent of a nod and wink—that "Segments consisting exclusively of *opinions* about cannabis or marijuana, and that do not infer use, are *not* prohibited."[98] Indeed, numerous segments targeting marijuana users are available on the Data Marketplace.[99]

106. Likewise, LiveRamp purports to prohibit segments regarding:[100]

a. Reproductive health and rights, pregnancy, and fertility;

b. Sexually transmitted diseases;

c. Mental health-related conditions;

d. Sexual orientation;

e. Conditions predominantly affecting or associated with children and not treated with over-the-counter medicine;

f. Information describing any individual's known health or medical condition(s), including Protected Health Information (PHI); and

g. Abortion.

---

[97] *Data Marketplace Segment Review and Approval*, LIVERAMP, https://docs.liveramp.com/connect/en/data-marketplace-segment-review-and-approval.html [https://perma.cc/ZP8M-VVAA] (emphasis in original).

[98] *LiveRamp's Data Marketplace Data Policy*, LIVERAMP, https://docs.liveramp.com/connect/en/liveramp-s-data-marketplace-data-policy.html [https://perma.cc/VQZ7-6B3B] (emphasis added).

[99] Jon Keegan and Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, THE MARKUP (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you [https://perma.cc/MUG2-N38J].

[100] *LiveRamp's Data Marketplace Data Policy*, LIVERAMP, https://docs.liveramp.com/connect/en/liveramp-s-data-marketplace-data-policy.html [https://perma.cc/VQZ7-6B3B].

Yet, LiveRamp simultaneously states that "[s]egments consisting exclusively of *opinions* about the health-related topics listed [above], and that do not infer the person has or has had the condition, are not prohibited," thereby allowing its customers to easily bypass its supposed restrictions.[101] In fact, as described above, LiveRamp' Data Marketplace offers for sale segments on many supposedly prohibited topics, such as mental health and reproductive health issues.

E. LiveRamp's "Third-Party Attribute Data Append" Is a Uniquely Invasive and Comprehensive Form of Surveillance.

107. LiveRamp offers a particularly invasive and comprehensive form of surveillance for sale through the Data Marketplace, known as the "Third-Party Attribute Data Append" (formerly known as the "Offline Data Marketplace").[102] Through this "Third-Party Attribute Data Append," LiveRamp connects its customers' first-party data—such as names, physical addresses, and email addresses—with "*all* of the currently-available data seller attributes" for the consumers associated with the data.[103] The customer then selects the segment data of interest and LiveRamp returns whatever "demographics and psychographic data" have been requested as an attachment to the original customer file.[104] In other words, LiveRamp appears to offer to those select customers "who meet certain criteria" access to *all* of the information about a particular, identifiable person available on its Data Marketplace.

108. LiveRamp provides a mockup image of an appended data file, labeled "INFUTOR SAMPLE LIVERAMP FILE."[105] The file shows the customer's data – names, addresses, emails, and phone numbers – and appended next to it, sweeping information about those individuals, including what style car they drive, details about their occupation, health, relationship status, finances, and shopping habits.[106]

---

[101] *Id.* (emphasis added).

[102] *Third-Party Attribute Data Append*, LIVERAMP, https://docs.liveramp.com/connect/en/offline-data-marketplace.html [https://perma.cc/37XV-4VHW].

[103] *Id*. (emphasis added).

[104] *Id*.

[105] *Id*.

[106] *Id*.

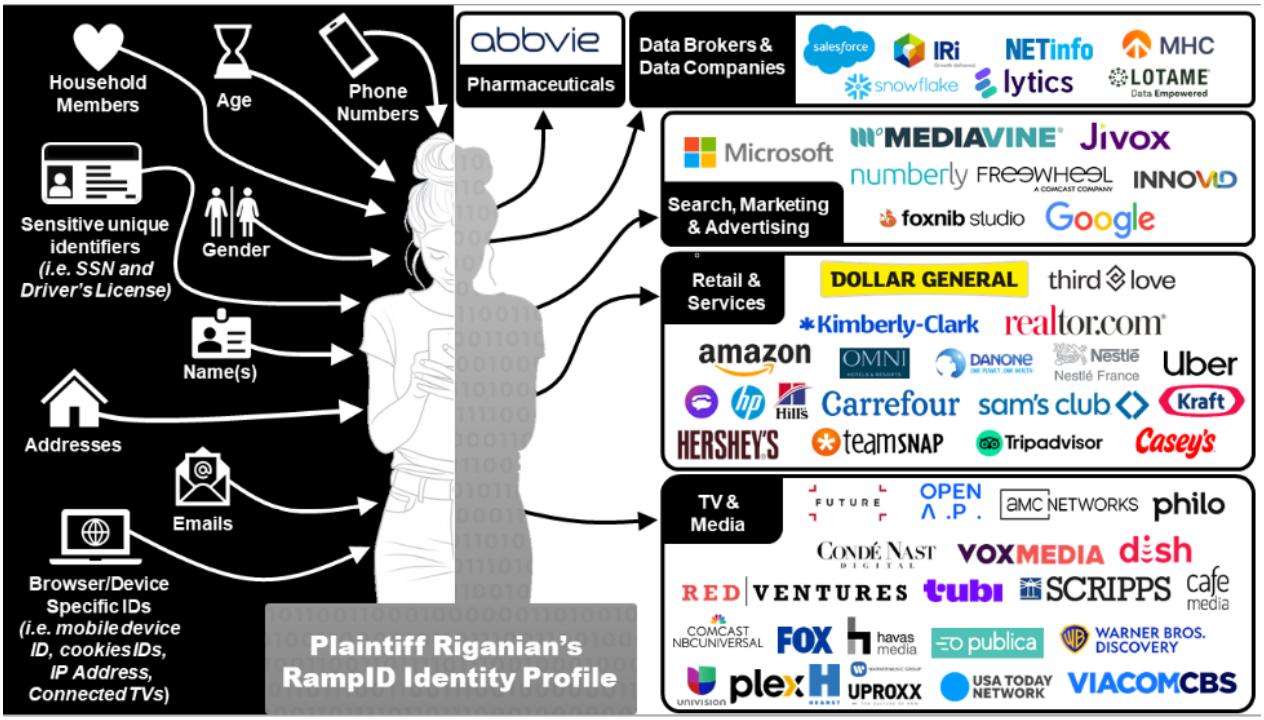
109. Given the scope and breadth of the information sold on the Data Marketplace, combined with LiveRamp's ability to track all U.S. consumers in real time and space on their devices through its RampID identity graph services, LiveRamp's sale of these highly detailed, personal, and sensitive "psychographic" profiles represents one of the most uniquely invasive and comprehensive forms of surveillance in modern history.

110. LiveRamp generates revenue from the Data Marketplace "through revenue-sharing arrangements with data owners that are monetizing their data assets on [the] marketplace."[107] LiveRamp profits greatly from the Data Marketplace; which, alone, generates over $100 million a year in revenue.[108]

111. Plaintiffs' knowledge regarding LiveRamp's collection and use of their data is described above at paragraphs 13–38. Based on current investigation, Plaintiffs cannot know the full extent of the specific information that has been bought or sold about them through LiveRamp's services or the Data Marketplace. However, the data collection, data brokering, and identity resolution practices described above exist to allow LiveRamp's customers to leverage those practices against individual consumers by targeting them *on an individual level* wherever they (or their devices) may be found online or offline. Plaintiff Riganian's RampID identity profile was shared, for example, with at least the following 62 third parties, though LiveRamp has not disclosed the specific data that was shared about Riganian with these third parties:

[107] LiveRamp, Form 10-K (Mar. 31, 2021), https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [https://perma.cc/KFM8-8KWQ].

[108] LiveRamp, Form 10-K (Mar. 31, 2023), https://investors.liveramp.com/node/18886/html [https://perma.cc/DS4R-64UB].



F. LiveRamp's Practices are Recognized as Highly Offensive and Threats to Individual Privacy.

112. LiveRamp originated as a notoriously privacy-invasive company known as "RapLeaf."[109] RapLeaf began, in 2006, as an online service through which people could rate each other based on their business transactions. The company soon began scraping information from social networks, voter-registration files, real estate records, and shopping histories, and matching that data to email addresses. Next, it "decided to connect its database of dossiers on people to cookies placed on those same individuals' computers."[110] This trove of sensitive data tied to each person allowed RapLeaf to begin selling sensitive segments to advertisers. A 2010 Wall Street Journal investigation found that few online tracking companies were willing to do what RapLeaf did – connect online trackers to personal information like names and emails.[111] In 2011, RapLeaf created

[109] *RapLeaf CEO Hoffman Discusses New LiveRamp Solution and Company Strategy*, ADEXCHANGER (July 8, 2011), https://www.adexchanger.com/data-exchanges/rapleaf-ceo-hoffman/ [https://perma.cc/A5PV-P97Y].

[110] Emily Steel, *A Web Pioneer Profiles Users by Name*, WALL STREET JOURNAL (Oct. 25, 2010), https://www.wsj.com/articles/SB10001424052702304410504575560243259416072 [https://perma.cc/M4G6-Q5GN].

[111] *Id.*

a data onboarding division named LiveRamp, which was acquired by Axciom in 2014, as discussed below. RapLeaf garnered significant public outrage over its privacy invasive and "creepy" practices.[112] The practices from which LiveRamp's business model originated were thus widely recognized as privacy-invasive and highly offensive to reasonable people since their inception.

113. LiveRamp is the new name of the company formerly called Acxiom, which was a data broker that owned "the world's largest commercial database on consumers," containing "information about 500 million active consumers worldwide, with about 1,500 data points per person."[113] LiveRamp was spun out into an independent company which was acquired by Acxiom in 2014 for $310 million.[114]

114. Acxiom was the subject of a notorious data breach in 2003 (1.6 billion unencrypted records stolen in a series of 137 attacks)[115] and embarrassing press in 2018 when Facebook (now Meta) stopped allowing advertisers to target audiences using third-party data brokers after the Cambridge Analytics scandal.[116] Acxiom was one of the data brokers Cambridge Analytics had used

---

[112] *Googlers Buy More Junk Food Than Micrsofties*, TECHCRUNCH (Mar. 22, 2011), https://techcrunch.com/2011/03/22/googlers-buy-more-junk-food-than-microsofties-and-why-rapleaf-is-creepy/ [https://perma.cc/8WFB-WASV] ("If you weren't creeped out by data-mining startup Rapleaf after reading about their ways in a relatively unsettling Wall Street Journal article published last October ('The San Francisco startup says it has 1 billion e-mail addresses in its database'), chances are you will be now."); *see also* Wikipedia, *RapLeaf*, https://en.wikipedia.org/wiki/RapLeaf [https://perma.cc/2EFJ-VKUM] ("Between 2007-2013, Rapleaf received significant backlash over the data collection practices and sale of individuals' personal information to advertisers." (citing sources)).

[113] Natasha Singer, *Acxiom, the Quiet Giant of Consumer Database Marketing*, N.Y. TIMES (June 16, 2012) https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/ZWL8-69J9].

[114] Wendy Parish, *Acxiom Acquires Liveramp To Expand Marketing Reach*, MARKETING DIVE (May 14, 2014), https://www.marketingdive.com/news/acxiom-acquires-liveramp-to-expand-marketing-reach/263131/ [https://perma.cc/PD5V-X9CA].

[115] Richard Behar, *Never Heard Of Acxiom? Chances Are It's Heard of You*, CNN MONEY (Feb. 23, 2004), https://money.cnn.com/magazines/fortune/fortune_archive/2004/02/23/362182/index.htm [https://perma.cc/TSL3-XSLT]; John Leyden, *Acxiom database hacker jailed for 8 years*, THE REGISTER (Feb. 23, 2006), https://www.theregister.com/2006/02/23/acxiom_spam_hack_sentencing/ [https://perma.cc/P645-3UVS].

[116] David Ingram and Julia Fioretti, *Facebook Cuts Ties to Data Brokers in Blow to Targeted Ads*, REUTERS (Mar. 29, 2018), https://www.reuters.com/article/us-facebook-privacy/facebook-cuts-ties-to-data-brokers-in-blow-to-targeted-ads-idUSKBN1H41KV [https://perma.cc/YZF5-LSHQ].

to target and manipulate U.S. voters in 2016[117] and repeatedly identified as one of the intended targets of Facebook's policy change.[118]

115. In early 2018, in part in response to the Cambridge Analytica scandal,[119] Acxiom Corporation reorganized into two business units: LiveRamp ("the identity cloud for transforming the world's data into value") and Acxiom Marketing Solutions ("the leading provider of data solutions for powering exceptional customer experiences").[120] LiveRamp received Acxiom's "identity assets," including the RampID identity graph system (then known as "IdentityLink"), the AbiliTec ID, and "Acxiom's TV integrations," thereby, according to the company, "creating the world's first truly end-to-end identity platform for people-based marketing."[121]

116. Acxiom Marketing Solutions (AMS) took on the rest of Acxiom's data and marketing business. In late 2018, facing intensified regulatory scrutiny in the wake of the Cambridge Analytica

---

[117] Natasha Lomas, *Cambridge Analytica's Nix Said It Licensed 'Millions Of Data Points' From Acxiom, Experian, Infogroup To Target US Voters*, TECHCRUNCH (June 6, 2018), https://techcrunch.com/2018/06/06/cambridge-analyticas-nix-said-it-licensed-millions-of-data-points-from-axciom-experian-infogroup-to-target-us-voters/ [https://perma.cc/33ZR-QBNE]; *see also* Nandini Jammi, (@nandoodles), X, https://twitter.com/nandoodles/status/1419580697833099268?lang=en [https://perma.cc/A42A-KY64].

[118] Kurt Wagner, *Facebook is Cutting Third-Party Data Providers Out of Ad Targeting to Clean Up Its Act*, VOX (Mar. 28, 2018), https://www.vox.com/2018/3/28/17174098/facebook-data-advertising-targeting-change-experian-acxiom [https://perma.cc/HQE7-FC5Q]; Nick Statt, *Facebook Will No Longer Allow Third-Party Data For Targeting Ads*, THE VERGE (Mar. 28, 2018), https://www.theverge.com/2018/3/28/17174854/facebook-shutting-down-partner-categories-ad-targeting-cambridge-analytica [https://perma.cc/YDF2-U8YZ]; Todd Spangler, *Facebook Says Info on Up to 87 Million Users Was 'Improperly' Shared With Cambridge Analytica*, VARIETY (Apr. 4, 2018), https://variety.com/2018/digital/news/facebook-87-million-users-cambridge-analytica-leak-1202743952/ [https://perma.cc/4YY6-2ND9].

[119] *See, e.g.*, Sara Fischer, *IPG to Acquire most of Acxiom for $2.3 billion*, AXIOS (July 2, 2018), https://www.axios.com/2018/07/02/interpublic-mediabrands-buys-majority-of-axciom-for-23-billion-dollars-1530570665; *see also* Mike Shields, *One of the data companies that Facebook just kicked off its platform is livid: 'We are getting thrown under the bus'*, BUSINESS INSIDER (Mar. 29, 2018), https://www.businessinsider.com/advertising-data-company-acxiom-is-livid-that-facebook-just-kicked-them-off-its-platform-2018-3.

[120] *Acxiom Realigns Portfolio to Drive Long-Term Success*, LIVERAMP (Feb. 6, 2018), https://investors.liveramp.com/news-releases/news-release-details/acxiom-realigns-portfolio-drive-long-term-success [https://perma.cc/WWT3-YUWY].

[121] *Id.*

scandal,[122] Acxiom sold AMS to The Interpublic Group of Companies Inc., a publicly traded group of advertising and marketing companies, and renamed itself LiveRamp Holdings, Inc.[123]

117. Both before its acquisition by legacy Acxiom in 2014 and especially since legacy Acxiom sold AMS and renamed itself LiveRamp in 2018, commentators have pointed to LiveRamp's tremendous capacity to inflict privacy harms. For example, in 2014, just as legacy Acxiom was acquiring LiveRamp, ProPublica pointed to LiveRamp as the reason "Why Online Tracking Is Getting Creepier,"[124] specifically referencing LiveRamp's merger of offline personal information and online identifiers. Quoting now-LiveRamp CEO Scott Howe, the article notes, "The marriage of online and offline is the ad targeting of the last 10 years on steroids."[125]

118. Critics, like then-Federal Trade Commission (FTC) Chairwoman Edith Ramirez, worried about LiveRamp's capacity to covertly control the public's experience of, and reaction to, the world around them: "Will these classifications mean that some consumers will only be shown advertisements for subprime loans while others will see ads for credit cards? . . . Will some be routinely shunted to inferior customer service?" LiveRamp's suggestion that its services can be used, for example, to exclude or "suppress" high risk prospective clients from insurance advertising indicates the answer to Ramirez's question is yes.[126]

119. These worries persist. In a 2022 article titled "These Companies Know When You're Pregnant—And They're Not Keeping It Secret," Gizmodo.com found *billions* of unique records for sale on LiveRamp's Data Marketplace purporting to identify people who were pregnant or interested

---

[122] Sara Fischer, *IPG to Acquire Most of Acxiom for $2.3 Billion*, AXIOS (July 2, 2018), https://www.axios.com/2018/07/02/interpublic-mediabrands-buys-majority-of-axciom-for-23-billion-dollars-1530570665 [https://perma.cc/PY59-8F9Y].

[123] *Acxiom Marketing Solutions Sale Now Complete*, LIVERAMP (Oct. 1, 2018), https://investors.liveramp.com/news-releases/news-release-details/acxiom-marketing-solutions-sale-now-complete [https://perma.cc/Y3EG-BXSZ].

[124] Julie Angwin, *Why Online Tracking is Getting Creepier*, PROPUBLICA (June 12, 2014), https://www.propublica.org/article/why-online-tracking-is-getting-creepier [https://perma.cc/KNS9-E5JN].

[125] *Id.*

[126] RampUp, *LiveRamp B2B: Identity Solutions are Open For Business | RampUp Conference*, YouTube at 33:48 (May 31, 2019), https://www.youtube.com/watch?v=M3nrB1rfKFE [https://perma.cc/6JXT-8VCP].

in becoming so: "32 different brokers across the U.S. selling access to the unique mobile IDs from some 2.9 billion profiles of people pegged as 'actively pregnant' or 'shopping for maternity products.' Also on the market: data on 478 million customer profiles labeled 'interested in pregnancy' or 'intending to become pregnant.'"[127] Gizmodo "was able to find each of these datasets up for sale through Liveramp, a company that, in part, functions as a clearinghouse and distribution hub [for] countless data brokers' wares."[128] Gizmodo also found that LiveRamp "did not put any restrictions on buying two-thirds of the databases." And "the minority that did come with purchasing conditions" simply "required authorization from Liveramp before purchasing.'"[129]

120. The article noted the intense state interest in this data:

> Pregnancy data is poised to be a huge boon for law enforcement in the post-Roe era. If you're a cop, [a] product manager said, it's as easy as "filling out [a data broker's] 'contact us' form and ask how much it costs. . . . [L]ikely, they'll say 'Put another zero after it, and see if we say yes.'"[130]

121. In 2020, Slate.com ranked LiveRamp as twelfth on its list of the thirty most "evil" (that is, harmful) tech companies. As summarized by Slate, "LiveRamp collects personal info like home values, credit card transactions, and health history from hundreds of millions of people in order to sustain the $100 billion online ad industry. Why do you keep seeing shoe ads all over the web, maybe even on this very page you're reading, after browsing for loafers on Amazon? These guys."[131]

122. One commentator pointed to data brokers like LiveRamp as "epitomiz[ing] the way 'online' and 'offline' behavior are being collapsed, even as there persists some sense that they are

---

[127] Shoshana Wodinsky and Kyle Barr, *These Companies Know When You're Pregnant—And They're Not Keeping It Secret*, GIZMODO (July 30, 2022), https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426 [https://perma.cc/FYW2-UL7B].

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *The Evil List*, SLATE (Jan. 15, 2020), https://slate.com/technology/2020/01/evil-list-tech-companies-dangerous-amazon-facebook-google-palantir.html [https://perma.cc/2MWZ-T7P5].

separate." A "profile about our viability as a consumer" constructed by LiveRamp "is a secret held against us . . . yet it *dictates the experiences we have* in the commercial world (*i.e.*, *everywhere*)."[132]

123. Like other new-model AdTech companies, LiveRamp markets itself as part of a new, "privacy protective" and "cookieless" advertising model that does not depend on tracking consumers' online activity through third-party cookies. But commentators argue that the "cookieless" future is even bleaker from a privacy perspective than the AdTech industry's past. "Cookieless" technologies like LiveRamp's generally depend on "first-party"—that is, consumer-provided—data such as email addresses and phone numbers.[133] "The proposed first-party identifiers essentially are more privacy-invasive than even cookies, and provide users with less transparency and control,"[134] These identifiers "create persistent, identifiable connections to people across activity on multiple devices," and, according to the privacy advocate, are "even more robust of an identifier than your actual name or other [personally-identifiable information]."[135]

124. Academic researchers likewise have raised the alarm about the false promises of "cookieless" advertising. The persistence of cookieless trackers like RampIDs "can last for a greater duration than third-party cookies, which users frequently delete."[136] Identity resolution services like LiveRamp's "allow[] advertisers to develop rich profiles of existing customers through pairing data purchased from data brokers but also non-customers across the open web."[137] And cookieless trackers "encourage circumvention of targeting restrictions by advertising platforms" because there is "no mechanism to verify how advertisers have segmented first-party data before importing into

---

[132] *Id.* (emphasis added).

[133] Kate Kaye, *After Winning The Battle Over Third-Party Cookie Tracking, Will Privacy Advocates Lose The Personal-Data Use War?*, DIGIDAY (Mar. 29, 2021), https://digiday.com/media/after-winning-the-battle-over-third-party-cookie-tracking-will-privacy-advocates-lose-the-personal-data-use-war [https://perma.cc/2NHE-HV93].

[134] *Id.*

[135] *Id.*

[136] Ido Sivan-Sevilla and Patrick T. Parham, *Toward (Greater) Consumer Surveillance in a 'Cookie-less' World: A Comparative Analysis of Current and Future Web Tracking Mechanisms*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Parham-Toward-Greater-Consumer-Surveillance-in-a-Cookie-less-World.pdf [https://perma.cc/FG6U-NEGM].

[137] *Id.*

these systems."[138] In short, "implementation of cookie-less tracking solutions by the AdTech complex potentially enables greater dynamic visibility on consumers, longer consumer tracking, and the assembling of more sensitive consumer profiles."[139] Far from the solution to the AdTech industry's privacy problems, LiveRamp represents the most recent and most sophisticated *evolution* of them.

125. The California Privacy Protection Agency—the nation's first dedicated privacy enforcement agency—has singled out LiveRamp's data collection and identification practices as particularly expansive, pointing to them as exemplifying invasive identity resolution practices, in particular the use of "myriad of different online identifiers for devices" that are "associate[d] with pseudonymous profiles."[140]

126. In 2024, the FTC sued LiveRamp business partner Avast for harming internet users by selling internet users' web browsing data to LiveRamp (among others) for LiveRamp's use, without internet users' knowledge or consent. According to the FTC:

> [From] May 2017 to April 2019, [Avast subsidiary] Jumpshot granted LiveRamp, a data company that specializes in various identity services, a "world-wide license" to use consumers' granular browsing information, including all clicks, timestamps, persistent identifiers, and cookie values, for a number of specified purposes. One specified purpose was "targeting, messaging and other data driven marketing activities served to consumers and businesses." Other terms appear to permit LiveRamp to use Jumpshot's consumer data to track and target consumers across multiple devices. . . . These provisions permit the targeting of Avast consumers using LiveRamp's ability to match Respondents' persistent identifiers to LiveRamp's own persistent identifiers, thereby associating data collected from Avast users with LiveRamp's data.

127. The FTC noted that "Re-identifiable browsing information," like that illegally sold to LiveRamp, "is sensitive data" and that Avast "had direct evidence that many consumers did not want their browsing information to be sold to third parties" like LiveRamp.[141]

---

[138] *Id.*

[139] *Id.*

[140] CALIFORNIA PRIVACY PROTECTION AGENCY, *Final Statement of Reasons*, https://cppa.ca.gov/meetings/materials/20230203_item4_fsor.pdf [https://perma.cc/9NX3-WC5Z] ("As demonstrated by LiveRamp's Subject Access Request Explanatory Information Document, businesses use a myriad of different online identifiers for devices that they can associate with pseudonymous profiles.").

[141] FEDERAL TRADE COMMISSION, *In the Matter of Avast Limited, et al.*, Complaint,

128. International privacy advocates have likewise decried LiveRamp's worldwide, deeply invasive surveillance practices. For example, on February 28, 2024, Open Rights Group ("ORG"), a UK-based digital privacy organization, submitted complaints about LiveRamp's practices to the UK Information Commissioner's Office ("ICO") and the French Commission Nationale de l'informatique et des Libertés ("CNIL") describing LiveRamp's practices as "more intrusive and pervasive than previous adtech technologies."[142] ORG states that LiveRamp's "new and dangerous technologies are an attempt to get around changes that limit the use of tracking cookies, and to make online advertising more intrusive rather than less."[143] ORG called on the ICO and the CNIL to "halt these new and dangerous technologies before they get out of hand."[144]

G. Effective Consent to LiveRamp's Practices is Impossible.

129. The long-established common law, statutory, and Constitutional rights to privacy are inherently and inextricably linked to fundamental cultural values of autonomy and freedom. The concept of "consent" reinforces these cultural values by functioning as a way for individuals to protect their privacy by exercising control over their personal information—what personal information organizations can collect, how they can use it, and to whom they can disclose it. LiveRamp conducts the business practices alleged in this complaint within a context and in a manner where consent from the persons whose data it assembles is not reasonably possible or practical, in fact does not occur, and for which, in light of the extent of the privacy rights that are violated by LiveRamp's business practices, no consent to such practices could be enforced as a matter of law.

---

https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-Avast.pdf [https://perma.cc/EVZ3-8JY5].

[142] *ORG Submits Complaints About Intrusive LiveRamp AdTech System*, OPEN RIGHTS GROUP (Feb. 28, 2024), https://www.openrightsgroup.org/press-releases/org-complaint-liveramp-adtech/ [https://perma.cc/8YDK-RU7G]; OPEN RIGHTS GROUP, Complaint to the ICO (Feb. 28, 2024), https://www.openrightsgroup.org/app/uploads/2024/02/ORG-complaint-FINAL.pdf [https://perma.cc/JU72-T4YP]; OPEN RIGHTS GROUP, Complaint to the CNIL (in French) (Feb. 28, 2024), https://www.openrightsgroup.org/app/uploads/2024/02/ORG-plainte.pdf [https://perma.cc/Z6WV-R5RV].

[143] *ORG Submits Complaints About Intrusive LiveRamp AdTech System*, OPEN RIGHTS GROUP (Feb. 28, 2024), https://www.openrightsgroup.org/press-releases/org-complaint-liveramp-adtech/ [https://perma.cc/8YDK-RU7G].

[144] *Id.*

130. Plaintiffs and Class members, like our society at large, have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet, with their personal information traveling through cyberspace every day. Because much of daily activities of life are now conducted online—whether financial, commercial, or social—Internet activity has become an "exhaustive chronicle" of one's life. The personal information necessary for these activities courses through the Internet as these activities take place, and, when aggregated, can provide deep insight into a person's thinking, acting, and being. Without an expectation of privacy on the Internet, there would functionally be no expectation of privacy anywhere. And, of course, there is no choice (other than homelessness) in having a physical address in the real world and other items of "offline PII" on which LiveRamp relies for its RampID product.

131. LiveRamp sits atop a complex data collection and processing apparatus, feeding its labyrinthine multinational data marketplace, making it impossible for ordinary persons to reasonably understand the true purpose and extent of LiveRamp's data collection, compiling of digital dossiers, and other data exploitation practices, which are opaque, if not invisible, to ordinary data subjects. Given the complexity and disguised nature of LiveRamp's collection and use of personal information, and the lack of any direct relationship between LiveRamp and the Plaintiffs and Class members, there is no reasonable basis for Plaintiffs and Class members to know the extent to which LiveRamp is obtaining their data, tracking them, and selling their data or services derived from their data. Indeed, even exceptionally well-informed people struggle to understand the full scope of these issues using publicly available information.

132. LiveRamp's presence on the Internet and in the digital world is ubiquitous, by design, and its data gathering activities are constant, vast, and encompass a massive swath of Internet activity. The breadth and complexity of sources from which LiveRamp compiles digital dossiers, or comprehensive identity profiles, on Class members is such that as a practical matter, Plaintiffs and Class members have no way of knowing—and thus no way of even being able to consent to—the actual scope of LiveRamp's conduct. Plaintiffs and Class members do not, merely by virtue of conducting the necessary activities of daily life, both online and in the physical world, consent to

constant and pervasive surveillance by LiveRamp and the creation of comprehensive identity profiles about them.

133. In as much as the Internet and digital existence has become integral to people's lives, its functioning and complexity with respect to personal information remains opaque to reasonably informed people. The Findings and Declarations of the California Privacy Rights Act (CPRA) notes that the "asymmetry of information" inherent in the "collect[ion] and use [of] consumers' personal information . . . makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses."[145] There is asymmetry of knowledge between LiveRamp and the data subjects it exploits, including Plaintiffs and Class members, in that LiveRamp has complete knowledge of its data collection and data exploitation practices, but Plaintiffs and Class members have no direct relationship with LiveRamp regarding these practices and no reasonable basis to discern those practices, nor the nature of the practices directed at them.

134. Plaintiffs and Class members cannot reasonably foresee all the ways in which LiveRamp may use the comprehensive identity profiles it is compiling on them. Plaintiffs and Class members have no way of knowing the specific third parties to which LiveRamp will provide their personal information or what those third parties will do with that information. Plaintiffs and Class members thus cannot provide knowing and informed consent to LiveRamp's dissemination of their personal information.

135. LiveRamp makes no pretense of having directly obtained consent from the persons whose data it gathers, including Plaintiffs and Class members. At no point during its process of collecting or processing personal information, compiling of dossiers, or selling services based on that personal information, does LiveRamp ever directly ask individuals for their consent. LiveRamp legally acknowledges this by virtue of its registration as a data broker wherein it admits it "does not have a direct relationship" with the subjects whose data it exploits. *See* Cal. Civ. Code § 1798.99.80. Instead, LiveRamp's fiction of consent depends on consent being given through each of its hundreds or thousands of "partner" websites and other online and offline services. But users of those services cannot reasonably be expected to read or comprehend each of the thousands of privacy policies they

[145] The California Privacy Rights Act of 2020, Sec. 2(F), https://thecpra.org/.

encounter. Nor should (or could) users reasonably anticipate the breadth with which their personal information is ultimately used – collected, collated, and compiled into dossiers, and sold to hundreds of data companies.

136. Nor have Plaintiffs and Class members manifested any form of consent indirectly to LiveRamp. LiveRamp publishes so-called privacy policies on its website, but these policies are not reasonably directed to Plaintiffs and Class members, all of whom lack any direct relationship with LiveRamp and have no reasonable insight into LiveRamp's data collection and data exploitation practices or how they may or may not be subject to such practices, and therefore there is no reasonable basis for Plaintiffs and Class members to be aware of LiveRamp's privacy policies or to have directed themselves to them. Plaintiffs and Class members are not legally subject to or governed by LiveRamp's published privacy policies. In any event, LiveRamp's privacy policies fail to disclose the nature or extent of the pervasive identity surveillance LiveRamp engages in, nor do they disclose the extent or sensitivity of the personal information available for sale through its Data Marketplace—indeed, LiveRamp's so-called privacy policies do not even *mention* the "Data Marketplace" at all.[146]

137. Even if Plaintiffs and Class members were to encounter LiveRamp's so-called privacy policies, the policies are themselves are insufficient to adequately inform Plaintiffs and Class members about the nature and extent of LiveRamp's data collection and data exploitation practices, especially with regard to their personal information. Plaintiffs and Class members are in the course of daily life barraged with thousands of pages of purported "terms and conditions" and "privacy policies" for online products and services. Computer science researchers have estimated that, based on the number of unique sites American Internet users visit annually, it would take the average Internet user between 181 to 304 hours to read the relevant privacy policies; this translates to approximately 72 billion hours per year for every U.S. Internet user to read all the privacy policies he or she encounters.[147] LiveRamp knows, or reasonably should know, that it is not reasonably

[146] *See, e.g.*, *California Privacy Notice*, LIVERAMP (Last Updated Oct. 15, 2024), https://liveramp.com/privacy/california-privacy-notice/ [https://perma.cc/GU7L-DKYM].

[147] *See* Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*. I/S

possible for Internet users to read or comprehend the thousands of privacy policies they encounter, including LiveRamp's privacy policies.

138. As privacy scholars have noted, issues that users must navigate to understand the significance of consent are too complex and the conditions surrounding consent too easy to manipulate for any purported consent to be informed and meaningful.[148] While it is well-known that many websites include "cookie popups" that purport to ask for consent for the website placing a cookie on the users' computer, in practice, most formulations of user control rights fail to sufficiently explain that cookie tracking leads to *profiling* based on information *derived* from user behavior. These practices, whether by LiveRamp or its "partners," fail to provide sufficient means to obtain the legally viable consent to LiveRamp's mass data collection, behavior tracking, and assembling of comprehensive identity profiles based on that data.

139. Neither LiveRamp's so-called privacy policies, nor the policies of third-party Internet publishers, could provide any reasonable basis for Plaintiffs and Class members to have consented to LiveRamp's data collection, compiling of comprehensive identity profiles, and other data exploitation practices, or to have waived their privacy rights, including to be free from LiveRamp's pervasive surveillance of them.

140. LiveRamp knows, or reasonably should know, that Internet users such as Plaintiffs and Class members have insufficient knowledge or basis to reasonably comprehend the extent to which LiveRamp is obtaining their data, tracking their activity, and compiling it into digital dossiers, nor the deeply invasive and detailed nature of those dossiers. LiveRamp makes no disclosure anywhere directly to Plaintiffs or Class members of these practices. To the extent Plaintiffs or Class members indirectly acknowledge to third parties the presence of some aspect of an isolated data

---

A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review Issue, at 17 (2008), https://kb.osu.edu/server/api/core/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content [https://perma.cc/X6R8-YXHW].

[148] *See* Alessandro Acquisti, Curtis Taylor et al., *The Economics of Privacy*, 54 J. ECON. LITERATURE 442 (2016), https://pubs.aeaweb.org/doi/pdfplus/10.1257/jel.54.2.442 [https://perma.cc/3KPV-5WHV]; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (2018); Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 NEW MEDIA & SOC'Y (2019), https://doi.org/10.1177/1461444819833331 [https://perma.cc/J8B4-K3ES].

collection practice, or tracking cookie on an individual website, such acknowledgement in no way does or could reflect any consent or sufficient understanding of LiveRamp's practices to connect their online identity to their offline identities and activities, and to surveil them on both for sale of their personal information in an international marketplace.

141. LiveRamp effectuates ongoing, comprehensive surveillance of Plaintiffs and Class members which grievously intrudes upon their privacy, and which inevitably results in the corrosion of their individual autonomy and the collective autonomy of the society at large. Ordinary people, such as Plaintiffs and Class members, do not and cannot possess an appropriate level of knowledge about the substantial threats that LiveRamp's surveillance poses to their own autonomy (in addition to lacking information sufficient to comprehend the nature and extent of LiveRamp's surveillance and its other implications).

142. The social harms posed by LiveRamp's conduct impair not only individual autonomy, but the collective autonomy of Plaintiffs and Class members, as all members of a society have an interest in the enforcement of privacy rights, freedom from surveillance, and preservation of autonomy. Evisceration of these privacy values inexorably leads to the abrogation of the autonomy and freedom of the citizenry which are essential to the proper functioning of democratic republics. These harms caused by LiveRamp far outweigh the commercial benefits that extend to a private corporation. In the context of LiveRamp's practices, valid consent from Plaintiffs and the Class members is not only absent, but not even possible.

143. Plaintiffs and Class members in fact have not waived their fundamental right to be free from the pervasive surveillance LiveRamp subjects them to. In any event, even if there were any basis to conclude that Plaintiffs and Class members could be considered to have waived their reasonable expectation of privacy with respect to LiveRamp's practices (and there is not), such waiver would be void and invalid as against public policy.

VIII. CLASS ALLEGATIONS

144. Plaintiffs bring this class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes, which are jointly referred to throughout this Complaint as the "Classes:"

United States Class:

All natural persons located in the United States whose personal information, or data derived from their personal information, was made available for sale or use through LiveRamp's RampID or Data Marketplace.

California Sub-Class:

All natural persons located in California whose personal information, or data derived from their personal information, was made available for sale or use through LiveRamp's RampID or Data Marketplace.

California Invasion of Privacy Act ("CIPA") Sub-Class:

All members of the California Sub-Class whose contents of their electronic communications were intercepted by LiveRamp or whose routing, addressing or signaling information was recorded by LiveRamp.

Electronic Communications Privacy Act ("ECPA") Sub-Class:

All members of the United States Class whose contents of their electronic communications were intercepted by LiveRamp.

145. Excluded from the Classes are the following individuals: officers and directors of LiveRamp and its parents, subsidiaries, affiliates, and any entity in which LiveRamp has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

146. Plaintiffs reserve the right to modify or amend the definition of each of the proposed Classes before the Court determines whether certification is appropriate.

147. This action readily satisfies the requirements set forth under Federal Rule of Civil Procedure 23:

a. Each Class is so numerous that joinder of all members is impracticable. Upon information and belief, Class members number in the millions.

b. There are questions of law or fact common to the Classes. These questions include, but are not limited to, the following:

1) Whether LiveRamp's acts and practices complained of herein amount to egregious breaches of social norms;

2) Whether LiveRamp acted intentionally in violating Plaintiffs' and Class members' privacy rights;

3) Whether LiveRamp was unjustly enriched as a result of its violations of Plaintiffs' and Class members' privacy rights;

4) Whether an injunction should issue; and

5) Whether declaratory relief should be granted.

c. Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and Class members did not consent to LiveRamp's interception, collection, analysis, and sale or their personal information, which acts form the basis for this suit.

d. Moreover, like all Class members, Plaintiffs suffer a substantial risk of repeated injury in the future. Plaintiffs continue to use devices that are capable of reporting personal information to LiveRamp. LiveRamp's actions have thwarted and continue to threaten Plaintiffs' (and Class members') ability to exercise control over their own privacy while using their devices. Because the conduct complained of herein is systemic, Plaintiffs and Class members face substantial risk of the same injury in the future. LiveRamp's conduct is common to Plaintiffs and Class members and represents a common pattern of conduct resulting in injury to all members of the Classes. Plaintiffs have suffered the harm alleged and have no interests antagonistic to any other Class member.

e. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs' interests do not conflict with the interests of Class members. Furthermore, Plaintiffs have retained competent counsel experienced in class action, consumer protection, and electronic privacy litigation. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Classes. Federal Rule of Civil Procedure 23(a)(4) and 23(g) are satisfied.

f. In acting as above-alleged, LiveRamp has acted on grounds generally applicable to the Classes, thereby making final injunctive relief and corresponding declaratory relief each appropriate with respect to the Classes as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for LiveRamp.

IX. CAUSES OF ACTION

First Cause of Action
Invasion of Privacy Under the California Constitution
(on behalf of the California Sub-Class)

148. Plaintiff Riganian and the California Sub-Class members repeat and reallege all preceding paragraphs contained herein.

149. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

150. The addition of the phrase "and privacy" occurred after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Proposition 11 was intended to curb businesses' control over the unauthorized collection and use of peoples' personal information, as the ballot argument stated:

> The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[149]

151. This amended constitutional provision addresses the concern over accelerating encroachment on personal freedom and security caused by increasing surveillance and data collection activity in contemporary society. Its proponents meant to afford individuals more measures of protection against this most modern threat to personal privacy:

> Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian.[150]

[149] Ballot Pamp., Proposed Stats. & Amends. To Cal. Const. With Arguments to Voters. Gen. Election *26 (Nov. 7, 1972).

[150] *Id.*

In recognizing these privacy rights, the California Constitution provides insight into and serves to define the nature of the reasonable expectation of privacy of an objectively reasonable California resident. In contravention to the California Constitution and the reasonable expectations of privacy of California residents, LiveRamp "stockpil[es] unnecessary information about [Class members] and [] misus[es]information gathered for one purpose in order to serve other purposes," creating "cradle-to-grave" profiles of Class members.

152. Plaintiff Riganian and the California Sub-Class members maintain a reasonable expectation of privacy in the conduct of their lives, including their internet browsing activities and in their electronic communications and exchange of personal information. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiff Riganian and the California Sub-Class members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiff Riganian's and the California Sub-Class members' private lives susceptible to unlawful observation and recording, capable of yielding a comprehensive and intrusive chronicle of Plaintiff Riganian's and the California Sub-Class members' lives. If Plaintiff Riganian and the California Sub-Class members cannot have a reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal information, they can have no reasonable expectation of privacy for virtually any facet of their lives.

153. LiveRamp, in violation of Plaintiff Riganian's and the California Sub-Class members' reasonable expectation of privacy, intercepts, collects, tracks, and compiles their internet activity and communications, and makes available for sale that data through third parties as well.

154. The nature and volume of the data collected is such that LiveRamp's practice of compiling comprehensive identity profiles violates Plaintiff Riganian's and the California Sub-Class members' reasonable expectation of privacy. Technological advances, such as LiveRamp's use of cookies, Client-Side Tags, and other means to track and compile internet activity and electronic communications, provide LiveRamp with the means to assemble a comprehensive chronicle of Plaintiff Riganian's and the California Sub-Class members' lives heretofore unseen. LiveRamp collects and compiles personal information such as Plaintiff Riganian's and the California Sub-Class

members' names, postal addresses, email addresses, phone numbers, cookies, mobile device IDs, and web browsing information. Such information is "personal information" under California law, which defines personal information as including "[i]nternet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

155. LiveRamp also collects and analyzes Plaintiff Riganian's and the California Sub-Class members' real-world offline activity and compiles computerized records of those activities. Plaintiff Riganian's and the California Sub-Class members do not and cannot know which specific real-world offline activities LiveRamp may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

156. LiveRamp's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. LiveRamp engages in dragnet-style collection and interception of Plaintiff Riganian's and the California Sub-Class members' Internet activity, including their communications with websites, without California Sub-Class members' knowledge or consent.

b. LiveRamp also collects details about Plaintiff Riganian's and the California Sub-Class members' *offline* activities. By its very nature, Plaintiff Riganian and the California Sub-Class members cannot be aware of or consent to this conduct.

c. LiveRamp creates comprehensive identity profiles based on this online and offline data, which constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California Constitution was created to constrain.

157. LiveRamp's amassing of electronic information reflecting highly detailed aspects of Plaintiff Riganian's and the California Sub-Class members' lives into dossiers, both directly and through providing access to its Data Marketplace, for future or present use, is in and of itself a violation of Plaintiff Riganian's and the California Sub-Class members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, these dossiers are and can be used to further invade Plaintiff Riganian's privacy, by, inter alia, allowing third parties to learn

intimate details of Plaintiff Riganian's and the California Sub-Class members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them. Additionally, as described above, the social harms posed by LiveRamp's conduct impair not only individual autonomy, but the collective autonomy of the California Sub-Class members, and autonomy is essential to the proper functioning of democratic republics.

158. Privacy advocates have repeatedly decried LiveRamp's practices as harmful and highly offensive. LiveRamp's conduct described herein has been the subject of scathing criticisms by government officials, academics, and technology journalists and of formal complaints to government authorities in the UK and France by privacy advocates.

159. Legislators have recognized the pernicious and privacy-invasive nature of LiveRamp's conduct as described herein. Senator Wyden, in urging the Consumer Financial Protection Bureau to take action against data brokers, stated that "[d]ata brokers are serving as shady middlemen to sell [consumers'] personal information without any legal protections" and that selling consumers' personal information and "giving them no choice in the matter, is an egregious abuse of consumers' privacy."[151] The FTC has also warned consumers about the "shadowy" "data broker ecosystem" where "companies have a profit motive to share data at an unprecedented scale and granularity," including a "staggering" amount of "highly personal information that people choose not to disclose even to family, friends, or colleagues."[152]

160. LiveRamp has violated Plaintiff Riganian's and the California Sub-Class members' reasonable expectation of privacy via LiveRamp's review, analysis, dissemination, and subsequent uses of Plaintiff Riganian's and California Sub-Class members' internet activity through LiveRamp's RampID identity graph system and Data Marketplace.

[151] December 8, 2021 Letter from Sen. Ron Wyden Letter to Rohit Chopra, Dir. of the Consumer Financial Protection Bureau, available at https://www.wyden.senate.gov/imo/media/doc/CFPB%20Letter%20120821.pdf.

[152] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data*, FEDERAL TRADE COMMISSION (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

161. LiveRamp's practices as alleged herein violate Plaintiff Riganian's and the California Sub-Class members' reasonable expectation of privacy, are highly offensive to a reasonable person, and constitute an egregious breach of the social norms.

162. LiveRamp's violation of various state and federal statutes, and its actions to enable others to violate various state and federal statutes relating to privacy protections are each an independent and egregious breach of social norms.

163. The California Constitution created an inalienable right to be free from pervasive electronic surveillance; Plaintiff Riganian and the California Sub-Class members are under no obligation to "opt out" of such violations of their constitutional privacy rights to stop LiveRamp's intrusions into their daily lives—that right inheres automatically for every California Sub-Class member.

164. The right to privacy in California's constitution creates a right of action for California residents against private entities such as LiveRamp. LiveRamp lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiff Riganian and the California Sub-Class members.

165. Plaintiff Riganian and the California Sub-Class members have been damaged by LiveRamp's invasion of their privacy and are entitled to just compensation and injunctive relief.

Second Cause of Action
Intrusion Upon Seclusion Under California Common Law
(on behalf of the United States Class)

166. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

167. California common law on intrusion upon seclusion is applicable for all members of the United States Class.

168. A plaintiff asserting a claim for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

169. Plaintiffs and the United States Class members maintain a reasonable expectation of privacy in the conduct of their lives, including their Internet browsing activities and in their electronic communications and exchange of personal information. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiffs and the

United States Class members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiffs' and the United States Class members' private lives susceptible to unlawful observation and recording that is capable of yielding a comprehensive and intrusive chronicle of Plaintiffs' and the United States Class members' lives. If Plaintiffs and the United States Class members cannot have a reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal information, they can have no reasonable expectation of privacy for virtually any facet of their lives.

170. LiveRamp, in violation of Plaintiffs' and the United States Class members' reasonable expectation of privacy intercepts, collects, tracks, and compiles their internet activity and communications, and makes available for sale that data through third parties as well.

171. The nature and volume of the data collected is such that LiveRamp's practice of compiling comprehensive identity profiles violates Plaintiffs' and the United States Class members' reasonable expectation of privacy. Technological advances, such as LiveRamp's use of cookies, Client-Side Tags, and other means to track and compile internet activity and electronic communications, provide LiveRamp with the means to assemble a comprehensive chronicle of Plaintiffs' and the United States Class members' lives heretofore unseen. LiveRamp collects and compiles personal information such as Plaintiffs' and the California Sub-Class members' names, postal addresses, email addresses, phone numbers, cookies, mobile device IDs, and web browsing information. Such information is "personal information" under California law, which defines personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

172. LiveRamp also collects and analyzes Plaintiffs' and the United States Class members' real-world offline activity and compiles computerized records of those activities. Plaintiffs and the United States Class members do not and cannot know which specific real-world offline activities LiveRamp may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

173. LiveRamp's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. LiveRamp engages in dragnet-style collection and interception of Plaintiffs' and Class members' Internet activity, including their communications with websites, without Class members' knowledge or consent.

b. LiveRamp also collects details about Plaintiffs' and the United States Class Members' *offline* activities. By its very nature, Plaintiffs and Class members cannot be aware of or consent to this conduct.

c. LiveRamp creates comprehensive identity profiles based on this online and offline data, which constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California Constitution was created to constrain.

d. LiveRamp violates federal and state statutes designed to protect Class Members' privacy, including but not limited to the causes of action alleged herein.

174. LiveRamp's amassing of electronic information reflecting highly detailed aspects of Plaintiffs' and the United States Class Members' lives into dossiers, both directly and through providing access to its Data Marketplace, for future or present use, is in and of itself a violation of Plaintiffs' and the United States Class members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, these dossiers are and can be used to further invade Plaintiffs' and the United States Class Members' privacy, by, inter alia, allowing third parties to learn intimate details of Plaintiffs' and the United States Class Members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control the dissemination and use of information about them. Additionally, as described above, the social harms posed by LiveRamp's conduct impair not only individual autonomy, but the collective autonomy of the United States Class members, and autonomy is essential to the proper functioning of democratic republics.

175. Privacy advocates have repeatedly decried LiveRamp's practices as harmful and highly offensive. LiveRamp's conduct described herein has been the subject of scathing criticisms

by government officials, academics, and technology journalists and of formal complaints to government authorities in the UK and France by privacy advocates.

176. Legislators have recognized the pernicious and privacy-invasive nature of LiveRamp's conduct as described herein. Senator Wyden, in urging the Consumer Financial Protection Bureau to take action against data brokers, stated that "[d]ata brokers are serving as shady middlemen to sell [consumers'] personal information without any legal protections" and that selling consumers' personal information and "giving them no choice in the matter, is an egregious abuse of consumers' privacy."[153] The FTC has also warned consumers about the "shadowy" "data broker ecosystem" where "companies have a profit motive to share data at an unprecedented scale and granularity," including a "staggering" amount of "highly personal information that people choose not to disclose even to family, friends, or colleagues."[154]

177. LiveRamp has violated Plaintiffs' and the United States Class members' reasonable expectation of privacy via LiveRamp's review, analysis, dissemination, and subsequent uses of Plaintiffs' and Class members' internet activity through LiveRamp's RampID identity graph system and Data Marketplace.

178. LiveRamp's practices as alleged herein violate Plaintiffs' and the United States Class members' reasonable expectation of privacy, are highly offensive to a reasonable person, and constitute an egregious breach of the social norms.

179. LiveRamp lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiffs and the United States Class members.

180. Plaintiffs and the United States Class members have been damaged by LiveRamp's invasion of their privacy and are entitled to just compensation and injunctive relief.

---

[153] December 8, 2021 Letter from Sen. Ron Wyden Letter to Rohit Chopra, Dir. of the Consumer Financial Protection Bureau, available at https://www.wyden.senate.gov/imo/media/doc/CFPB%20Letter%20120821.pdf.

[154] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data*, FEDERAL TRADE COMMISSION (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

181. As a result of LiveRamp's actions, Plaintiffs and the United States Class members seek injunctive relief, in the form of LiveRamp's cessation of tracking practices in violation of Plaintiffs' and Class members' rights, and destruction of all personal information obtained in violation of Plaintiffs' and Class members' rights.

182. As a result of LiveRamp's actions, Plaintiffs and the United States Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because LiveRamp's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and the United States Class members and made in conscious disregard of their rights. Punitive damages are warranted to deter LiveRamp from engaging in future misconduct.

183. Plaintiffs and the United States Class members seek restitution for the unjust enrichment obtained by LiveRamp as a result of unlawfully collecting Plaintiffs' and the United States Class members' personal information. These intrusions are highly offensive to a reasonable person. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and the United States Class members' personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of LiveRamp's conduct is the fact that LiveRamp's principal goal is and was to surreptitiously monitor Plaintiffs and the United States Class members and to allow third parties to do the same.

184. The threat posed by advancements in technology and the ability to create detailed dossiers therefrom was recognized half a century ago by Professor Arthur R. Miller.[155] With monumental increases in technologies, Professor Miller's alarm 50 years ago about technology's assault on privacy has now taken on special urgency: precisely the concerns he warned of have come to fruition in LiveRamp's conduct. Through this lawsuit, Plaintiffs and the United States Class members seek to vindicate their common law right against LiveRamp's ongoing assault on their privacy.

[155] *See generally* Arthur R. Miller, *The Assault on Privacy* 24–54 (1971).

Third Cause of Action
Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630 to 638
(on behalf of the CIPA Sub-Class)

185. Plaintiff Riganian and the California Invasion of Privacy Act ("CIPA") Sub-Class members repeat and reallege all preceding paragraphs contained herein.

186. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code § 630 ("Legislative declaration and intent").

California Penal Code § 631

187. California Penal Code § 631(a) prohibits, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section. . . .

Under this section of CIPA, a defendant must show it had the consent of all parties to a communication and that its actions are not done "in *any* unauthorized manner." The California Supreme Court has emphasized CIPA's privacy-protective objective. *See Flanagan v. Flanagan*, 27 Cal. 4th 766, 769, 41 P.3d 575, 577 (2002) ("The purpose of [CIPA] was to protect the right of privacy by, among other things, requiring that all parties consent to a recording of their conversation.").

188. Speaker of the California Assembly, Jesse Unruh, who introduced CIPA, urged that the law "represents an important advance in California law protecting the inherent rights of our citizens to privacy in their personal affairs. It is far stronger than the laws of many states in this field,

and much tougher than the proposed federal eavesdropping legislation."[156] He further emphasized that the law would act as "a powerful deterrent to those who wiretap illegally for profit."[157]

189. LiveRamp deploys "Client-Side Tags" and "Enhanced Client-Side Tags" on websites to gather data on consumers' online activities. LiveRamp's Client-Side Tags automatically "capture," or intercept, the URLs of the web pages visited, the exact date and time of the visit, and communications with websites such as "page views," "ad views," "adding items to cart," or "completing a transaction." LiveRamp deploys these tags by surreptitiously using "image tags," or pixels, to insert code into Plaintiff Riganian's browser that intercepts the contents of Plaintiff Riganian's and CIPA Sub-Class members' communications with websites while those communications are in transit.[158] This captured data then goes through LiveRamp's recognition process to match the website visitors to their specific RampIDs and to link that data with LiveRamp's persistent identity profile on Plaintiff Riganian and CIPA Sub-Class members. At all relevant times, LiveRamp's tracking and interceptions of Plaintiff Riganian's and CIPA Sub-Class members' internet communications was without authorization and consent from Plaintiff Riganian and CIPA Sub-Class members. The interception by LiveRamp in the aforementioned circumstances were unlawful and tortious.

190. LiveRamp's interception of communications also occurred in a manner that was not authorized by Plaintiff Riganian, who did not consent to LiveRamp's tracking of her identity and communications content across broad swaths of the Internet.

191. The communications intercepted by LiveRamp include "contents" of electronic communications made from Plaintiff Riganian and CIPA Sub-Class members to websites other than those operated by LiveRamp in the form of:

a. the URL strings with which Internet users are viewing and interacting with; and,

---

[156] July 31, 1967, Letter from Rep. Jesse M. Unruh to then California governor Ronald Reagan urging him to sign CIPA into law.

[157] *Id.*

[158] *Implementation Methods for Client-Side Tags*, LIVERAMP, https://docs.liveramp.com/identity/en/implementation-methods-for-client-side-tags.html [https://perma.cc/S9CC-SEZ4].

b. the precise activity that users are engaged in, *e.g.*, "adding items to a cart"; "completing a transaction."

192. The URLs being browsed by the Internet user constitute contents of communications as they encompass the substance, purpose, or meaning of a user's Internet communication. Likewise, "adding items to a cart" and "completing a transaction" constitute contents of communications, as they communicate the user's intent to a websites. For example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that book on hold. There is no question that wiretap of such a phone conversation would intercept the "contents" of a communication. Actions demonstrating purchase intent on websites are no different.

193. On information and belief, LiveRamp intercepted detailed URLs of webpages Plaintiff Riganian viewed, including URLs revealing searches she performed, and communications with websites related to purchases or intended purchases, including product page visits and adding items to a cart. Examples of webpages that Plaintiff Riganian interacted with for which the contents of their communications were intercepted by LiveRamp include, but are not limited, to those listed in paragraph 26 above.

194. On information and belief, LiveRamp intercepted the contents of Plaintiff Riganian's communications with numerous websites in a similar manner and through various apps, including but not limited to those listed in paragraph 26 above.

195. Additionally, LiveRamp's "ATS.js" JavaScript Code, implemented through its Enhanced Client-Side Tag,[159] intercepts personal information, such as email addresses entered into forms when signing in to LiveRamp "partner" websites, phone numbers, and other customer identifiers communicated by Plaintiff Riganian and Class members to websites, and uses that information to create a universal identifier that is unambiguously linked to a specific person for use for targeting and manipulation by LiveRamp's clients.

[159] "The eCST module for ATS.js implementation of the Enhanced Client-Side Tag can be placed on web and mobile web owned and operated properties." *LiveRamp's Client-Side Tags*, LIVERAMP, https://docs.liveramp.com/safe-haven/en/implementing-liveramp-s-client-side-tag.html [https://perma.cc/8T3Z-3HEP].

196. The ATS.js JavaScript code uses so-called "event listeners" to detect specific types of contents of communications from Plaintiff Riganian and Class members to websites and intercept those contents and simultaneously transmit them to LiveRamp. Specifically, once ATS.js has been deployed on a website or in an app, ATS.js listens for and intercepts email addresses, phone numbers, or other customer identifiers communicated to that website or app.

197. LiveRamp's "ATS Mobile SDK" includes largely identical functionality that is deployed on mobile devices. On information and belief, and on the basis of the information contained in the "mobile_pel_requests" file sent to Plaintiff Riganian, LiveRamp's ATS Mobile SDK was deployed on Plaintiff Riganian's devices and intercepted the contents of her communications with mobile applications on her phone without her consent, as described herein.

198. On information and belief, LiveRamp intercepted the email addresses and phone numbers Plaintiff Riganian communicated to webpages and mobile applications through the use of the ATS.js JavasScript and ATS Mobile SDK. These email addresses are "contents" when sent as part of a sign-in. Examples of webpages that Plaintiff Riganian interacted with for which the contents of their communications were intercepted by LiveRamp via these ATS trackers include, but are not limited, to those listed in paragraph 26 above.

199. LiveRamp's non-consensual tracking of Plaintiff Riganian's and CIPA Sub-Class members' internet communications was designed to attempt to learn at least some meaning of the content in the URLs, their email addresses and phone numbers input during sign-in processes, and other data interception.

200. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, LiveRamp's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The computer codes and programs LiveRamp used to track Plaintiff Riganian's and CIPA Sub-Class members' communications;

b. Plaintiffs' and CIPA Sub-Class members' browsers and mobile applications;

c. Plaintiffs' and CIPA Sub-Class members' computing and mobile devices;

d. The computer codes and programs used by LiveRamp to effectuate its tracking and interception of Plaintiff Riganian and CIPA Sub-Class members'; and

e. The plan LiveRamp carried out to effectuate its tracking and interception of Plaintiff Riganian's and CIPA Sub-Class members' communications.

201. Plaintiff Riganian and CIPA Sub-Class members have suffered loss by reason of these violations, including, but not limited to, violations of their rights to privacy and loss of value in their personally identifiable information.

202. Pursuant to California Penal Code § 637.2, Plaintiff Riganian and CIPA Sub-Class members have been injured by the violations of California Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

California Penal Code § 638.51

203. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

204. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

205. Courts have repeatedly recognized that in the internet era pen registers can take the form of software and, as a result, private companies and persons have the ability gather the same electronic information as law enforcement. The California legislature does not limit its prohibition on installing pen registers to law enforcement.

206. LiveRamp's Client-Side Tags, Enhanced Client-Side Tags, and ATS.js JavaScript code and SDK functionality constitute "pen registers" because they are "devices" or "processes" that "record" "addressing or signaling information,"—such as Plaintiff Riganian's and Class members' IP addresses and electronic device identification numbers including Identifiers for Advertisers (IDFAs) and Android Advertising IDs (AAIDs) as well as cookie IDs—from the electronic communications transmitted by their smartphones and desktop computers. To the extent the URLs, email addresses, and phone numbers intercepted by LiveRamp's Client-Side Tags,

Enhanced Client-Side Tags, and ATS.js JavaScript code and SDK functionality do not constitute contents of communications, they constitute routing, addressing, or signaling data.

207. LiveRamp was not authorized by any court order to use a pen register to record Plaintiff Riganian's and Class members' routing, addressing, or signaling information.

208. LiveRamp uses pen registers to collect such information *en masse* from class members as a non-party to their communications with websites, for the express purpose of creating comprehensive identity profiles on Plaintiff Riganian and Class members and facilitating the tracking of all of their online activity and making that information available to third parties. The interception of phone numbers and email addresses is done for the express purpose of personally identifying Plaintiff Riganian and Class members and using that personally identifying information to link Plaintiff Riganian's and Class members' online activities to the permanent profiles LiveRamp maintains on them. The data LiveRamp collects and aggregates for use with its RampID through its pen registers constitutes "unique fingerprinting," thereby providing unique information normally within the domain of law enforcement officers with a warrant.

209. As a direct and proximate result of LiveRamp's conduct, Plaintiff Riganian and Class members suffered losses and were damaged in an amount to be determined at trial.

Fourth Cause of Action
Violation of the Federal Wiretap Act, 18 U.S.C. § 2510, et. seq.
(on behalf of the ECPA Sub-Class)

210. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

211. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 (ECPA), prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

212. The Wiretap Act protects both the sending and receipt of internet communications. The Act was amended by ECPA because it had "not kept pace with the development of communications and computer technology [or] changes in the structure of the telecommunications industry."[160] In introducing the bill that became the ECPA, Senator Patrick Leahy explained that

[160] Electronic Communications Privacy Act, Sen. Rep. 99-541 at 2 (1986).

"the law must protect private communications from interception by an eavesdropper, whether the eavesdropper is a corporate spy, a police officer without probable cause, or just a plain snoop."[161] ECPA received strong support from privacy advocates, law enforcement and the technology industry. Industry advocates pointed out that "the protections in [the ECPA] should, if broadly applied, prevent customers from losing their privacy rights when they resort, as they must in this day and age, to third-party processors and transmitters of data."[162]

213. 18 U.S.C. § 2520(a) provides a private right of action to any person whose "wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the Wiretap Act.

214. As described above, LiveRamp intercepts Plaintiffs and ECPA Sub-Class members' communications with websites by deploying "Client-Side Tags" and "Enhanced Client-Side Tags" on websites to gather data on consumers' online activities.

215. LiveRamp's actions in intercepting and tracking user communications while they were browsing the internet was intentional. On information and belief, LiveRamp is aware that it is intercepting communications in these circumstances and has taken no remedial action.

216. LiveRamp's interception of internet communications that Plaintiffs and ECPA Sub-Class members were sending and receiving was done contemporaneously with the sending and receipt of those communications.

217. The communications intercepted by LiveRamp include "contents" of electronic communications made from Plaintiffs and ECPA Sub-Class members to websites other than those operated by LiveRamp in the form of:

a. the full URL strings with which Internet users are viewing and interacting with, as well as the referrer URL; and

b. the precise activity that users are engaged in, *e.g.*, "adding items to a cart"; and "completing a transaction."

[161] Congressional Record, Senate, September 19, 1985 at 24365-71.

[162] Electronic Communications Privacy Act, Hearing Before the House Committee on the Judiciary on H.R. 3378 at 74.

218. The detailed URLs being browsed by the Internet user and data entered by the user into forms on the website constitute contents of communications as they encompass the substance, purpose, or meaning of a users' Internet communication. Likewise, "adding items to a cart" and "completing a transaction" constitute contents of communications, as they communicate the user's intent to a website. For example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that book on hold. There is no question that a wiretap of such a phone conversation would intercept the "contents" of a communication. Actions demonstrating purchase intent on websites are no different.

219. LiveRamp's "ATS.js" JavaScript Code, implemented through its Enhanced Client-Side Tag,[163] intercepts personal information, such as email addresses and phones, communicated by Class members to websites, and uses that information to create a universal identifier that is unambiguously linked to a specific person for use for targeting and manipulation by LiveRamp's clients. The ATS.js JavaScript Code employs so-called "event listeners" to eavesdrop on Class members' sensitive communications with websites—specifically LiveRamp's code intercepts identifiers such as emails addresses or phone numbers that class members communicate to websites.

220. LiveRamp's "ATS Mobile SDK" includes largely identical functionality that is deployed on mobile devices. On information and belief, and on the basis of the information contained in the "mobile_pel_requests" file sent to Plaintiff Riganian, LiveRamp's ATS Mobile SDK was deployed on Plaintiff Riganian's devices and intercepted the contents of her communications with mobile applications on her phone without her consent, as described herein.

221. On information and belief, LiveRamp intercepted the email addresses and phone numbers Plaintiffs Riganian and Spurgeon communicated to webpages and mobile applications through the use of the ATS.js JavaScript and ATS Mobile SDK. These email addresses are "contents" when sent as part of a sign-in. Examples of webpages that Plaintiff Riganian interacted

[163] "The eCST module for ATS.js implementation of the Enhanced Client-Side Tag can be placed on web and mobile web owned and operated properties." *LiveRamp's Client-Side Tags*, LIVERAMP, https://docs.liveramp.com/safe-haven/en/implementing-liveramp-s-client-side-tag.html [https://perma.cc/8T3Z-3HEP].

with for which the contents of their communications were intercepted by LiveRamp via these ATS trackers include, but are not limited to, a subset of those listed in paragraphs 26 and 37 above.

222. As soon as LiveRamp has captured a class member's email address and phone number and linked that browsing session to its internal profile of the user in its systems, that user's identity becomes immediately available to be broadcast to tens of thousands of participants in the "Real-Time Bidding" ecosystem, which allows for real-time targeting and manipulation of class members.

223. Plaintiffs and ECPA Sub-Class members do not, by virtue of simply signing in to services that they use throughout the course of their daily lives, consent to the creation of an unavoidable and permanent internet identification number that follows them throughout their lives and that can be used by commercial or political actors to surveil and manipulate them.

224. Security researchers have determined that LiveRamp is the most prolific third-party exfiltrator of email addresses from websites in the United States, with trackers on such prominent websites as WebMD and Fox News.[164]

225. On information and belief, LiveRamp intercepted detailed URLs of web pages Plaintiffs viewed, including URLs revealing searches Plaintiffs performed, and communications with websites related to purchases or intended purchases, including product page visits, purchase intent signals or add-to-cart actions.

226. The transmission of data between Plaintiffs and ECPA Sub-Class members on the one hand and the websites on which LiveRamp tracked and intercepted their communications on the other, without authorization were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

227. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

[164] Asuman Senol et al., *Leaky forms: A study of email and password exfiltration before form submission*, 31st USENIX Security Symposium (USENIX Security 22) (2022) (pp. 1813-1830), https://www.usenix.org/system/files/sec22-senol.pdf [https://perma.cc/DA7D-PWCX].

a. The computer codes and programs LiveRamp used to track Plaintiffs and ECPA Sub-Class members' communications, including JavaScript code;

b. Plaintiffs' and ECPA Sub-Class members' browsers and mobile applications;

c. Plaintiffs' and ECPA Sub-Class members' computing and mobile devices;

d. The computer codes and programs used by LiveRamp to effectuate its tracking and interception of Plaintiffs' and Class members' communications; and

e. The plan LiveRamp carried out to effectuate its tracking and interception of Plaintiffs' and ECPA Sub-Class members' communications while browsing the internet.

228. LiveRamp, in its conduct alleged here, was not providing an "electronic communication service," as that term is defined in 18 U.S.C. § 2510(12) and is used elsewhere in the Electronic Communications Surveillance Act.

229. LiveRamp was not acting as an Internet Service Provider (ISP).

230. LiveRamp was not an authorized party to the communication, because Plaintiffs and ECPA Sub-Class members were unaware of LiveRamp's interception of their communications with websites and did not knowingly send any communication to LiveRamp. LiveRamp could not manufacture its own status as a party to Plaintiffs' and ECPA Sub-Class members' communications with others by surreptitiously intercepting those communications.

231. As described above, the communications between Plaintiffs and ECPA Sub-Class members on the one hand, and websites on the other, were simultaneous to, but separate from, the channel through which LiveRamp acquired the contents of those communications; and involved the re-direction of the communications content to LiveRamp.

232. The interception by LiveRamp in the aforementioned circumstances was performed for the secondary and independent purpose of committing tortious acts in violation of the law, specifically:

a. Violating the California Constitution's prohibition on the compiling of electronic dossiers, which dossiers are enriched by the contents of the communications intercepted by LiveRamp, as described herein; and

b. Violating the tort of intrusion upon seclusion by using the contents of the intercepted communications to create detailed profiles on Plaintiffs and ECPA Sub-Class members, and then making those profiles available through LiveRamp's RampID and Data Marketplace, as described herein.

233. On information and belief, LiveRamp was aware that its conduct was tortious and intended to violate Plaintiffs' and ECPA Sub-Class members' privacy and other rights.

234. The 1) compiling of electronic dossiers, which dossiers are enriched by the contents of the communications intercepted by LiveRamp in violation of the California Constitution, and 2) use of the contents of the intercepted communications to facilitate the creation of detailed profiles on Plaintiffs and ECPA Sub-Class members and then make those profiles available through LiveRamp's RampID and Data Marketplace, in violation the tort of intrusion upon seclusion, are illegitimate purposes under the ECPA.

235. Consent is not a defense where a "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Subsequent use or disclosure of the contents of the intercepted communications for the purpose of further invading Plaintiffs' and ECPA Sub-Class members' privacy is a tortious act that satisfies this exception to consent. In addition to having the intent of profiting from the sale of Plaintiffs' and ECPA Sub-Class members' personal information, LiveRamp knowingly and intentionally invaded Plaintiffs' privacy through intercepting their communications and using the fruits of those interceptions to further invade Plaintiffs' and ECPA Sub-Class members' privacy through pervasive identity surveillance and the facilitation of the purchase and sale of their detailed personal information through the Data Marketplace.

236. After intercepting the communications, LiveRamp then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

237. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and ECPA Sub-Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same

or similar conduct by LiveRamp in the future; and reasonable attorney's fees and other litigation costs reasonably incurred.

Fifth Cause of Action
Unjust Enrichment under California Common Law
(on behalf of the United States Class, or in the alternative on behalf of the California Sub-Class)

238. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

239. California common law on unjust enrichment is applicable for all members of the United States Class.

240. In the alternative, Plaintiffs allege unjust enrichment under California law on behalf of the California Sub-Class.

241. LiveRamp has wrongfully and unlawfully trafficked in Plaintiffs' and the United States Class members' personal information and other personal information without their consent and for substantial profits.

242. Plaintiffs' and the United States Class members' personal information and data have conferred an economic benefit on LiveRamp.

243. LiveRamp has been unjustly enriched at the expense of Plaintiffs and Class members, and the company has unjustly retained the benefits of its unlawful and wrongful conduct.

244. It would be inequitable and unjust for LiveRamp to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

245. Plaintiffs and the United States Class members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that LiveRamp obtained as a result of its unlawful and wrongful conduct.

246. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant. LiveRamp has been unjustly enriched by virtue of its violations of Plaintiffs' and United States Class members' legally protected rights to privacy as alleged herein, entitling Plaintiffs and United States Class members to restitution of LiveRamp's enrichment. "[T]he

consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." Restatement (Third) of Restitution § 1, cmt. a.

247. The elements for a claim of unjust enrichment are (1) receipt of a benefit and (2) unjust retention of the benefit at the expense of another. The doctrine applies where a plaintiff, while having no enforceable contract, nonetheless has conferred a benefit on defendant which defendant has knowingly accepted under circumstances that make it inequitable for the defendant to retain the benefit without paying for its value.

248. It is a longstanding principle of law embodied in the Restatement (Third) of Restitution and Unjust Enrichment (2011) that a person who is unjustly enriched at the expense of another may be liable for the amount of the unjust enrichment even if the defendant's actions caused the plaintiff no corresponding loss. Where "a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss or, in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust . . . [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched." Rest., Restitution, § 1, com. e.

249. The comments to the Restatement (Third) explicitly recognize that an independent claim for unjust enrichment may be predicated on a privacy tort. Restatement (Third) of Restitution and Unjust Enrichment § 44 cmt. b ("Profitable interference with other protected interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement").

250. Because "[a] person is not permitted to profit by his own wrong," *id.* § 3, "[g]ains realized by misappropriation, or otherwise in violation of another's legally protected rights, must be given up to the person whose rights have been violated." *Id.* ch. 5, introductory note. These principles are deeply ingrained in California law. California courts have long recognized a common law claim based on unjust enrichment. In determining the remedy for such claims, California courts apply principles found in the Restatement.

251. The unauthorized use of Plaintiffs' and United States Class members' information for profit entitles them to profits unjustly earned.

252. LiveRamp has unjustly profited from tracking, disclosing, and profiting from Plaintiffs and United States Class members' internet activity and real-world activity to third parties without Plaintiffs and United States Class members' knowledge or consent.

253. Plaintiffs did not provide authorization for the use of their personal information, nor did LiveRamp provide them with control over its use to produce revenue. This unauthorized use of their information for profit entitles Plaintiffs to profits unjustly earned.

254. It would be unjust and inequitable to allow LiveRamp to profit from its violation of Plaintiffs' and United States Class members' Constitutional, common law, and statutory rights as described herein.

255. LiveRamp was aware of the benefit conferred by Plaintiffs. Indeed, LiveRamp's Data Marketplace is premised entirely on the sale of such data to third parties. LiveRamp acted in conscious disregard of the rights of Plaintiffs and United States Class members and should be required to disgorge all profit obtained therefrom to deter LiveRamp and others from committing the same unlawful actions again.

Sixth Cause of Action
Declaratory Judgment that LiveRamp Wrongfully Accessed, Collected, Stored, Disclosed, Sold, and Otherwise Improperly Used Plaintiffs' Personal Information and Injunctive Relief
(on behalf of all Classes)

256. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

257. The gravamen of this controversy lies in LiveRamp's collection, tracking, and analysis of Plaintiffs' and Class members' personal information and behavior, building dossiers based on that information, and providing that information to third parties. Plaintiffs and Class members never consented to, or were even aware of, LiveRamp's conduct described herein.

258. LiveRamp's misconduct has put Plaintiffs' and Class members' privacy and autonomy at risk, and violated their dignitary rights, privacy, and economic well-being.

259. Accordingly, Plaintiffs seek appropriate declaratory relief, and injunctive relief as prayed for below.

X. PRAYER FOR RELIEF

260. Plaintiffs respectfully request that the Court:

A. Issue an order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, that Plaintiffs' attorneys shall be appointed as Class Counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

B. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

C. Appoint Plaintiffs to represent the Classes;

D. Appoint undersigned counsel to represent the Classes;

E. Enter Judgment in favor of Plaintiffs and the Class members against LiveRamp awarding damages, including statutory damages, punitive damage, and/or nominal damages, to Plaintiffs and the Class members, in an amount according to proof at trial, including interest thereon;

F. Enter Judgment in favor of Plaintiffs and Class members against LiveRamp awarding unjust enrichment and/or restitution of LiveRamp's ill-gotten gains, revenues, earnings, or profits that it derived, in whole or in part, from its unlawful collection and use of Plaintiffs' and Class members' personal information, in an amount according to proof at trial;

G. Enter Declaratory Judgment in favor of Plaintiffs and Class members against LiveRamp pursuant to 28 U.S.C. § 2201, declaring that LiveRamp's conduct is unlawful as alleged herein.

H. Permanently restrain LiveRamp, and its officers, agents, servants, employees and attorneys, from intercepting, tracking, collecting, or compiling the personal information of Plaintiffs and Class members as alleged herein;

I. Award Plaintiffs and Class members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

J. Grant Plaintiffs and Class members further equitable, injunctive, declaratory, or other relief as the Court deems appropriate.

XI. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all issues so triable.

Dated: January 24, 2025

Respectfully Submitted,

/s/ *Michael W. Sobol*
Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Linnea D. Pittman (*pro hac vice* forthcoming)
lpittman@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

/s/ Jason O. Barnes
Jason "Jay" O. Barnes (*pro hac vice* forthcoming)
jaybarnes@simmonsfirm.com
An V. Truong (*pro hac vice* forthcoming)
atruong@simmonsfirm.com
Sona R. Shah (*pro hac vice* forthcoming)
sshah@simmonsfirm.com
SIMMONS HANLY CONROY LLP
12 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: 212.784.6400
Facsimile: 212.213.5949

Attorneys for Plaintiffs and the Proposed Classes

ATTESTATION

Pursuant to Civil Local Rule 5.1 regarding signatures, I attest that concurrence in the filing of this document has been obtained from the other signatories.

Dated: January 24, 2025

/s/ *Michael W. Sobol*
Michael W. Sobol
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

3159767.1